NOTICE OF FILING

This document was lodged electronically in the FEDERAL COURT OF AUSTRALIA (FCA) on 1/03/2022 9:31:43 AM AEDT and has been accepted for filing under the Court's Rules. Details of filing follow and important additional information about these are set out below.

Details of Filing

Document Lodged:	Statement of Claim - Form 17 - Rule 8.06(1)(a)
File Number:	NSD134/2022
File Title:	CHIEF EXECUTIVE OFFICER OF THE AUSTRALIAN TRANSACTION REPORTS AND ANALYSIS CENTRE v CROWN MELBOURNE LIMITED ACN 006 973 262 & ANOR
Registry:	NEW SOUTH WALES REGISTRY - FEDERAL COURT OF AUSTRALIA

Dated: 1/03/2022 9:38:35 AM AEDT Registrar

Important Information

As required by the Court's Rules, this Notice has been inserted as the first page of the document which has been accepted for electronic filing. It is now taken to be part of that document for the purposes of the proceeding in the Court and contains important information for all parties to that proceeding. It must be included in the document served on each of those parties.

The date and time of lodgment also shown above are the date and time that the document was received by the Court. Under the Court's Rules the date of filing of the document is the day it was lodged (if that is a business day for the Registry which accepts it and the document was received by 4.30 pm local time at that Registry) or otherwise the next working day for that Registry.

Form 17
Rule 8.05(1)(a)

STATEMENT OF CLAIM

FEDERAL COURT OF AUSTRALIA
DISTRICT REGISTRY: NEW SOUTH WALES
DIVISION: COMMERCIAL AND CORPORATIONS **NO NSD** **OF 2022**

CHIEF EXECUTIVE OFFICER OF THE AUSTRALIAN TRANSACTION REPORTS AND ANALYSIS CENTRE
APPLICANT

CROWN MELBOURNE LIMITED
ACN 006 973 262
FIRST RESPONDENT

BURSWOOD NOMINEES LTD ATF THE BURSWOOD PROPERTY TRUST TRADING AS CROWN PERTH
ACN 078 250 307
SECOND RESPONDENT

INDEX

Filed on behalf of the Applicant, the Chief Executive Officer of the Australian Transaction Reports and Analysis Centre

Prepared by: Sonja Marsic
AGS lawyer within the meaning of s 55I of the *Judiciary Act 1903*

Address for Service:
Australian Government Solicitor,
Level 10, 60 Martin Pl, Sydney 2000
sonja.marsic@ags.gov.au

File ref: 22001484

Telephone: 02 9581 7505
Lawyer's Email:
sonja.marsic@ags.gov.au

PARTIES

The Chief Executive Officer of AUSTRAC

1. The Applicant is the Chief Executive Officer (**CEO**) of the Australian Transaction Reports and Analysis Centre (**AUSTRAC**) an office established under s211 of the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (Cth) (the **Act**).

2. The AUSTRAC CEO may apply for a civil penalty order by reason of s176 of the Act.

3. The objects of the Act, among others, include to provide for measures to detect, deter and disrupt money laundering, the financing of terrorism and other serious financial crimes.

Particulars

Section 3(1)(aa) of the Act.

4. The objects of the Act, among others, also include to promote confidence in the Australian financial system through the enactment and implementation of controls and powers to detect, deter and disrupt money laundering, terrorism financing and other serious crimes.

Particulars

Section 3(1)(ad) of the Act.

5. The AUSTRAC CEO may, by writing, make rules prescribing matters required or permitted by any provision of the Act to be prescribed by the rules.

Particulars

Section 229 of the Act.

Anti-Money Laundering and Counter-Terrorism Financing Rules 2007 (the **Rules**).

Crown Melbourne

6. The First Respondent, Crown Melbourne Limited (**Crown Melbourne**):is and was at all material times a company incorporated in Australia;

   a. is and was at all material times a person within the meaning of s5 of the Act;

   b. at all material times has carried on activities or business through a permanent establishment in Australia for the purposes of the Act;

   c. is and was at all material times a reporting entity within the meaning of s5 of the Act; and

   d. provides designated services to customers within the meaning of s6 of the Act, including:

      i. **Item 6, table 1** – making a loan, where the loan is made in the course of carrying on a loans business.

      ii. **Item 7, table 1** – in the capacity of a lender for a loan, allowing the borrower to conduct a transaction in relation to the loan, where the loan was made in the course of carrying on a loans business.

      iii. **Item 31, table 1** – in the capacity of a non-financier carrying on a business of giving effect to remittance arrangements, accepting an instruction from a

transferor entity for the transfer of money or property under a designated remittance arrangement.

iv. **Item 32, table 1** - in the capacity of a non-financier carrying on a business of giving effect to remittance arrangements, making money or property available, or arranging for it to be made available, to an ultimate transferee entity as a result of a transfer under a designated remittance arrangement.

v. **Item 1**, **table 3** – receiving or accepting a bet placed or made by a person, where the service is provided in the course of carrying on a gambling business.

vi. **Item 4, table 3** – paying out winnings in respect of a bet, where the service is provided in the course of carrying on a gambling business.

vii. **Item 6, table 3** – accepting the entry of a person into a game where: that game is played for money or anything else of value; the game is a game of chance or of mixed chance and skill; the service is provided in the course of carrying on a gambling business; and the game is not played on a gaming machine located at an eligible gaming machine venue.

viii. **Item 7, table 3** – exchanging money or digital currency for gaming chips / tokens / betting instruments, where the service is provided in the course of carrying on a business.

ix. **Item 8, table 3** – exchanging gaming chips / tokens / betting instruments for money or digital currency, where the service is provided in the course of carrying on a business.

x. **Item 9, table 3** – paying out winnings, or awarding a prize, in respect of a game where: that game is played for money or anything else of value; the game is a game of chance or of mixed chance and skill, the service is provided in the course of carrying on a gambling business, and; the game is not played on a gaming machine located at an eligible gaming machine venue.

xi. **Items 11 to 13, table 3** – in the capacity of account provider:

A. opening an account; or

B. allowing a person to be a signatory on an account; or

C. allowing a transaction to be conducted in relation to an account,

where the account provider is a person who provides a service covered by items 1, 2, 3, 4, 6, 7, 8 or 9 above, and the purpose, or one of the purposes, of the account is to facilitate the provision of a service covered by items 1, 2, 3, 4, 6, 7, 8 or 9 above, and the service is provided in the course of carrying on a business.

xii. **Item 14, table 3** – exchanging one currency (whether Australian or not) for another (whether Australian or not), where the exchange is provided by a person who provides a service covered by items 1, 2, 3, 4, 6, 7, 8 or 9 above, and the service is provided in the course of carrying on a business.

Crown Perth

7. The Second Respondent, Burswood Nominees Ltd atf the Burswood Property Trust trading as Crown Perth (**Crown Perth**):

a. is and was at all material times a company incorporated in Australia;

b. is and was at all material times a person within the meaning of s5 of the Act;

c. at all material times has carried on activities or business through a permanent establishment in Australia for the purposes of the Act;

d. is and was at all material times a reporting entity within the meaning of s5 of the Act; and

e. provides designated services to customers within the meaning of s6 of the Act, including each of the designated services pleaded at paragraph 6e.

Crown Resorts Limited

8. Crown Resorts Limited (**Crown Resorts**) is the ultimate holding company for the First and Second Respondents.

Particulars

See paragraphs 157 to 160.

Between March 2017 and November 2020, the Chief Legal Officer of Crown Resorts was also the AML/CTF Compliance Officer (**AMLCO**) for both Crown Melbourne and Crown Perth.

Rule 8.5 of the Rules.

THE ML/TF RISKS FACED BY CROWN

9. Money laundering:

a. is the process of turning the proceeds of crime into money that appears to be legitimate;

b. aims to conceal the identity, source, and destination of illicitly-obtained money; and

c. aims to move illicitly-obtained money through a legitimate business or transfer system.

10. The Act requires reporting entities to identify, mitigate and manage the money laundering and terrorism financing (**ML/TF**) risks reasonably faced with respect to the provision of designated services to customers.

Particulars

See paragraphs 29 to 46 below.

11. The ML/TF risks faced by Crown Melbourne and Crown Perth arise from both:

a. the provision of gaming services (table 3, s6 designated services); and

b. the movement of money facilitated by the provision of financial services (table 1, s6 designated services).

The risk-based approach and ML/TF risk

12. The Act and Rules permit a risk-based approach to the identification, mitigation and management of ML/TF risks by reporting entities.

13. When determining and putting in place appropriate risk-based systems and controls, a reporting entity must have regard to the nature, size and complexity of its business and the type of ML/TF risk it might reasonably face.

Particulars

Rules 8.1.3 and 9.1.3 of the Rules.

14. In identifying, mitigating and managing ML/TF risks, a reporting entity must consider the risk posed by:

    a. its customer types, including any politically exposed persons (**PEPs**);

    b. the types of designated services it provides;

    c. the methods by which it delivers designated services (which is known as **channel risk**); and

    d. the foreign jurisdictions with which it deals.

Particulars

Sections 84(2)(a) and (c), 85(2)(a) and (c) of the Act and rules 8.1.4 and 9.1.4 of the Rules.

The nature, size and complexity of Crown Melbourne's and Crown Perth's business and ML/TF risks reasonably faced

15. Crown Melbourne and Crown Perth facilitate high volume, high frequency and high value designated services, 24 hours a day, 7 days a week, including across international borders.

16. The proceeds of crime are often in cash.

17. The casinos operated by Crown Melbourne and Crown Perth are vulnerable to laundering of proceeds from a range of serious and organised crime activities including drug and tobacco offences, tax evasion, tax and welfare fraud and illegal gambling because:

    a. they are cash intensive businesses; and

    b. the source and ownership of cash is harder to trace compared to other forms of money.

18. A customer of Crown Melbourne and Crown Perth can move money through different designated services, including by:

    a. transferring money through cash, casino value instruments (**CVIs**), such as chips and tickets, and gaming accounts (table 3, s6 services);

    b. transferring money to or from their own gaming account (items 32 and 31, table 1, s6 services, respectively, or **remittance services**); and

    c. drawing on or redeeming credit provided by Crown Melbourne or Crown Perth (item 7, table 1, s6 services - **loans or credit**), which could be used for table 3, s6 gaming services and could involve remittance services.

19. The movement of money through different designated services by Crown Melbourne and Crown Perth customers can involve:

    a. long and complex transaction chains; and

    b. multiple channels, including non-face-to-face channels

which make it difficult to understand the purpose of transactions, the beneficial owner of funds or the ultimate beneficiary of value moved.

20. Crown Melbourne and Crown Perth provided both gaming and financial services to higher risk customers, including:

    a. through junket channels and VIP Programs, as described at paragraphs 464 to 583 below;

    b. to customers from foreign jurisdictions, including international VIPs; and

    c. to PEPs, including foreign PEPs.

21. Crown Melbourne and Crown Perth dealt with customers, including higher risk customers, through agents and third parties.

Money laundering vulnerabilities and typologies

22. The Financial Action Task Force (**FATF**), the Asia/Pacific Group on Money Laundering (**APG**) and AUSTRAC have identified significant money laundering vulnerabilities, related case studies and 'ML/TF typologies' specific to casinos.

23. **ML/TF typologies** are the various methods that criminals use to conceal, launder or move illicit funds.

24. The FATF, APG and AUSTRAC publications describe the following vulnerabilities and ML/TF typologies:

    a. As casinos are cash intensive businesses, they are vulnerable to **structuring**. This is the deliberate division of a large amount of cash into smaller deposits to avoid the reporting threshold in s43 of the Act.

    b. **Cuckoo smurfing** is a method of money laundering used by criminals to move funds across borders and make money generated by their illegal activities appear to have come from a legitimate source.

    c. Cuckoo smurfing is facilitated by professional money laundering syndicates who work with a corrupt remitter based overseas:

        i. The corrupt remitter accepts an instruction from a customer to make a payment to an Australian-based beneficiary customer.

        ii. The corrupt remitter hijacks the money transfer coming into Australia in order to place funds in the Australian-based beneficiary account which are sourced from criminal activity.

        iii. A **smurf or third party agent**, deposits cash into Australian bank accounts on behalf of a money laundering syndicate controller.

        iv. The international transfer is offset without the physical movement of funds.

    d. Casinos accepting cash or third party deposits for customers are vulnerable to cuckoo smurfing.

    e. Designated services facilitated through junkets are vulnerable to cuckoo smurfing and structuring. Junket operators may act as remitters and may facilitate cuckoo smurfing.

    f. **Offsetting** enables the international transfer of value without actually transferring money. This is possible because the arrangement involves a financial credit and debit

(offsetting) relationship between two or more persons operating in different countries. Criminals can exploit offsetting to conceal the amount of illicit funds transferred, obscure the identity of those involved and avoid reporting to AUSTRAC.

g. Gaming accounts are vulnerable to offsetting.

h. **Loans or credit** can also be used to launder funds. Loans can be taken out as a cover for laundering criminal proceeds under the guise of repayments, including by lump sum cash payments, smaller structured cash amounts or offsetting.

i. Customers of casinos may seek to use third parties to obtain designated services on their behalf. Third parties may also seek to deposit money into a customer's gaming account. A customer may seek to transfer money from their gaming account to a third party. The involvement of **third-parties in transactions such as these** can distance customers from illicit funds, disguise ownership of funds and complicate asset confiscation efforts by authorities. Third parties can also be used as **smurfs**.

j. Money deposited with a casino or exchanged for CVIs (including chips and tickets) and then withdrawn with **minimal or no gaming activity** may appear to have a legitimate origin, even though very little money was actually risked.

k. Gaming losses sustained by a customer, even if minimal, can give the incorrect appearance that the customer is engaging in genuine gaming activity.

l. Gaming involving **high turnover or high losses** may indicate unusual or suspicious activity and may raise questions about the customer's source of wealth or funds.

m. Gaming involving **escalating rates of high turnover or high losses** may indicate unusual or suspicious activity and may raise questions about the customer's source of wealth or funds.

n. **High turnover** offers further opportunities for the **placement and layering of illicit funds**. This is a particular problem with junkets, where funds are pooled and the payment of winnings is facilitated by the junket operator. The problem is exacerbated where cash can be brought into private gaming rooms by unknown persons who are not junket players.

o. Games that have a **low house edge** can be attractive to money launderers, as they offer the opportunity to launder large amounts with minimised losses. The house edge is a term used to describe the mathematical advantage that a game, and therefore the casino, has over the customer with play over time.

p. Where games permit **even-money wagering** (such as roulette and baccarat), two customers can cover both sides of an even bet to give the appearance of legitimate gaming activity while minimising losses.

q. Games that permit **rapid turnover of cash or CVIs** are vulnerable to money laundering. This vulnerability is exacerbated where the game is automated and not face-to-face.

r. **Chips and other CVIs are highly transferable** and may be handed over to third parties or removed from casinos and used as currency by criminal groups, or taken out of the jurisdiction as a means of transferring value. The chips may be returned to the casino by third parties and cashed out, including in amounts below a reporting threshold.

s. **Purchase of CVIs such as tickets** means a money laundering typology whereby individuals purchase CVIs from other customers using illegitimate funds and claim winnings from the Cage.

t. The acceptance of **bank cheques** made out to casinos may facilitate money laundering. Bank cheques are essentially anonymised, as the casino cannot identify the source of the funds. A customer may use the bank cheque to purchase CVIs, which may then be converted to cash.

u. **Bill Stuffing** involves a customer putting cash into an electronic gaming machine, collecting tickets with nominal gaming activity, then cashing out or asking for a cheque.

v. Casinos are also vulnerable to **refining**, which involves changing of an amount of money from smaller denomination bills into larger ones.

w. **Loan sharking** is when a person lends money in exchange for its repayment at an excessive interest rate, and may involve intimidating or illegal methods to obtain repayment. Although there is no specific offence for loan sharking, the conduct of a loan shark may breach other laws.

x. Money may be **parked** in gaming accounts. Parking of illicit money puts distance between the act or acts that generated the illicit funds and the ultimate recipients of those funds, making it harder to understand or trace the flow of money. Gaming accounts can be used to park or hide funds from law enforcement and relevant authorities.

Particulars

Vulnerabilities of Casinos and Gaming Sector, FATF/APG Report, (March 2009), (**FATF/APG Casino Typologies Report**).

Detect and Report Cuckoo Smurfing: Financial Crime Guide, (June 2021), AUSTRAC and Fintel.

Junket Tour Operations in Australia: Money Laundering and Terrorism Financing Risk Assessment, (2020), AUSTRAC (**AUSTRAC Junket Assessment**).

FATF - Risk Based Approach Guidance for Casinos, (October 2008) (**FATF RBA Guidance**).

25. At all times, Crown Melbourne and Crown Perth were exposed to the vulnerabilities and ML/TF typologies pleaded at paragraph 24 with respect to the provision of designated services.

26. By reason of the matters pleaded at paragraphs 15 to 25, the provision of designated services by Crown Melbourne and Crown Perth involves higher ML/TF risks.

THE AML/CTF PROGRAM

27. A reporting entity must not commence to provide a designated service to a customer unless the reporting entity has adopted and maintains an anti-money laundering and counter-terrorism financing program (**AML/CTF program**), within the meaning of s83 of the Act, that applies to the reporting entity.

Particulars

Sections 81(1) and 83 of the Act and rule 1.2.1 of the Rules.

28. An AML/CTF program is relevantly defined to include a standard AML/CTF program and a joint AML/CTF program.

Particulars

Section 83(1)(a) and (b) of the Act.

Standard AML/CTF program

29. A standard AML/CTF program is:

a. a written program that applies to a particular reporting entity; and

b. divided into Part A (general) and Part B (customer identification).

Particulars

Section 84(1) of the Act.

30. Part A of a standard AML/CTF program is a part the primary purpose of which is to:

a. identify; and

b. mitigate; and

c. manage;

the risk the reporting entity may reasonably face that the provision by the reporting entity of designated services at or through a permanent establishment of the relevant reporting entity in Australia might (whether inadvertently or otherwise) involve or facilitate money laundering or financing of terrorism (**ML/TF risk**).

Particulars

Section 84(2)(a) of the Act.

31. Part A of a standard AML/CTF program must comply with the Rules.

Particulars

Section 84(2)(c) of the Act.

32. Part B of a standard AML/CTF program is a part the sole or primary purpose of which is to set out the applicable customer identification procedures (**ACIPs**) for the purposes of the application of the Act to customers of the reporting entity.

Particulars

Section 84(3)(a) of the Act.

33. Part B of a standard AML/CTF program must comply with the Rules.

Particulars

Section 84(3)(b) of the Act.

Joint AML/CTF Program

34. A joint AML/CTF program is:

a. a written program that applies to each reporting entity that belongs to a particular designated business group (**DBG**); and

b. divided into Part A (general) and Part B (customer identification).

Particulars

Section 85(1) of the Act.

35. At all times on and from 1 March 2016, Crown Melbourne and Crown Perth were members of a DBG.

Particulars

The definition of designated business group is in s5 of the Act.

36. Part A of a joint AML/CTF program is a part the primary purpose of which is to:

a. identify; and

b. mitigate; and

c. manage

the risk each of those reporting entities within a DBG may reasonably face that the provision by the relevant reporting entity of designated services at or through a permanent establishment of the relevant reporting entity in Australia might (whether inadvertently or otherwise) involve or facilitate money laundering or terrorism financing (as defined in paragraph 30, **ML/TF risk**).

Particulars

Section 85(2)(a) of the Act.

37. Part A of a joint AML/CTF program must comply with the Rules.

Particulars

Section 85(2)(c) of the Act.

38. Part B of a joint AML/CTF program is a part the sole or primary purpose of which is to set out the ACIPs for the purposes of the application of the Act to customers of the reporting entities in the DBG.

Particulars

Section 85(3)(a) of the Act.

39. Part B of a joint AML/CTF program must comply with the Rules.

Particulars

Section 85(3)(b) of the Act.

The Rules - The Part A Program

40. Sections 84(2)(c) and 85(2)(c) of the Act require a Part A program to comply with requirements specified in the Rules including:

a. rules 8.1.3 and 9.1.3 which require a reporting entity, when putting in place appropriate risk-based systems or controls, to have regard to the nature, size and complexity of the

reporting entity's business and the type of ML/TF risk that the reporting entity might reasonably face;

b. rules 8.1.4 and 9.1.4 which require a reporting entity in identifying its ML/TF risk to consider the following factors:

   i. its customer types, including any PEPs;

   ii. the types of designated services it provides;

   iii. the methods by which it delivers designated services; and

   iv. the foreign jurisdictions with which it deals;

c. rules 8.1.5 and 9.1.5 which require the Part A program to be designed in a way so as to enable the reporting entity to:

   i. understand the nature and purpose of the business relationship with its customer types;

   ii. understand the control structure of non-individual customers;

   iii. identify significant changes in ML/TF risk for the purposes of its Part A and Part B programs, including (a) risks identified by consideration of the factors in rule 8.1.4 and (b) risks arising from changes in the nature of the business relationship, control structure, or beneficial ownership of its customers;

   iv. recognise such changes in ML/TF risk for the purposes of the requirements of its Part A and Part B programs;

   v. identify, mitigate and manage any ML/TF risk arising from: (a) all new designated services prior to introducing them to the market; (b) all new methods of designated service delivery prior to adopting them; (c) all new or developing technologies used for the provision of a designated service prior to adopting them; and (d) changes arising in the nature of the business relationship, control structure or beneficial ownership of its customers;

d. rules 8.4.1 and 9.4.1 which require a reporting entity's Part A program to be approved by its governing board and senior management. Part A must also be subject to the ongoing oversight of the reporting entity's board and senior management;

e. rules 8.5.1 and 9.5.1 which require the Part A program to provide for the reporting entity to designate a person as the AMLCO at the management level; and

f. rules 8.6 and 9.6 which require that the Part A program be subject to regular independent review and in the manner provided for under the rule.

The Rules - Carrying out the applicable customer identification procedures and the Part B Program

41. Reporting entities are required to carry out ACIPs to identify customers, generally before commencing to provide a designated service.

Particulars

Section 32 of the Act.

42. Exceptions to this general rule apply in relation to some designated services provided by Crown Melbourne and Crown Perth.

Particulars

Chapter 10 of the Rules made under s39 of the Act.

43. Chapter 10 of the Rules relevantly provide:

    a. The obligation in s32 of the Act does not apply in respect of a designated service under items 1, 2, 4, 6, 7, 8 or 9 of table 3, s6 that involves an amount of less than $10,000.

Particulars

Rule 10.1.3 of the Rules.

    b. The obligation in s32 of the Act does not apply in respect of a designated service under items 1, 2, 4, 6 or 9 of table 3, s6 that involves:

        i. an amount of less than $10,000; and

        ii. the customer giving or receiving only gaming chips or tokens.

Particulars

Rule 10.1.4 of the Rules.

    c. The exemptions in rules 10.1.3 and 10.1.4 do not apply in circumstances where a reporting entity determines in accordance with its enhanced customer due diligence (**ECDD**) program that it should obtain and verify any know your customer (**KYC**) information in respect of a customer in accordance with its customer identification program.

Particulars

Rule 10.1.5 of the Rules.

44. Rule 14.4 of the Rules relevantly provides that the obligation in s32 of the Act does not apply to a designated service under item 14, table 3, s6 (foreign exchange):

    a. where the value of the currency is less than $1,000 (in Australian dollars or foreign equivalent); and

    b. the proceeds and/or funding source of the designated service is in the form of physical currency.

45. The exemption in rule 14.4 does not apply where a reporting entity determines in accordance with its ECDD program that it should obtain and verify any KYC information about a customer in accordance with its customer identification program.

Particulars

Rule 14.5 of the Rules.

46. Sections 84(3)(b) and 85(3)(b) of the Act require a Part B program to comply with the requirements specified in Chapter 4 of the Rules which include the following:

    a. Relevantly, rule 4.1.3 provides that for the purposes of meeting the requirements of Chapter 4 of the Rules, a reporting entity must consider the risk posed by the following factors when identifying its ML/TF risk:

        i. its customer types, including any PEPs;

        ii. its customers' sources of funds and wealth;

iii. the nature and purpose of the business relationship with its customers;

iv. the types of designated services it provides;

v. the methods by which it delivers designated services (or channel);

vi. the foreign jurisdictions with which it deals.

b. Rule 4.2.2 requires a Part B program to include appropriate risk-based systems and controls that are designed to enable the reporting entity to be reasonably satisfied that a customer who is an individual is the individual that he or she claims to be.

c. Rule 4.2.3 requires a Part B program to include a procedure for the reporting entity to collect, at a minimum, the following KYC information about an individual: full name, date of birth, and residential address.

d. Rule 4.2.5 requires a Part B program to include appropriate risk-based systems and controls for the reporting entity to determine whether any other additional KYC information will be collected in addition to this information.

e. Rule 4.2.6 requires a Part B program to include a procedure for the reporting entity to verify, at a minimum, the customer's full name and either the customer's date or birth or their residential address.

f. Rule 4.2.8 requires a Part B program to include appropriate risk-based systems and controls for the reporting entity to determine whether any additional KYC information should be verified.

g. Rules 4.2.10 to 4.2.14 set out 'safe harbour' ACIPs for individual customers whose risk is medium or lower.

h. Part 4.11 makes provision for ACIPs for agents of customers.

i. Rule 4.11.2 requires a Part B program to include a procedure for the reporting entity to collect, at a minimum:

i. the full name of each individual who purports to act for or on behalf of the customer with respect to the provision of a designated service by the reporting entity; and

ii. evidence (if any) of the customer's authorisation of any such individual.

j. Rule 4.11.3 requires a Part B program to include appropriate risk-based systems and controls for the reporting entity to determine whether and to what extent it should verify the identity of individuals (either the customer or their purported agents).

k. Part 4.13 of the Rules provides for the collection and verification of PEP information.

l. Rule 4.13.1 requires a Part B program to include appropriate risk-management systems to determine whether a customer or beneficial owner is a PEP; either before the provision of a designated service to the customer or as soon as practicable after the designated service has been provided.

m. For domestic PEPs and international organisation PEPs, rule 4.13.2 requires a Part B program to determine whether the person is of high ML/TF risk.

n. If the person is a domestic PEP or international organisation PEP who has been assessed as posing a high ML/TF risk, or if the person is a foreign PEP, then rules

4.13.2(3) and 4.13.3 respectively require a Part B program to include appropriate risk-management systems for the reporting entity to undertake each of the following steps:

i. comply with identification requirements in rules 4.2.3 to 4.2.9 of the Rules in the case of a beneficial owner;

ii. obtain senior management approval before establishing or continuing the business relationship;

iii. take reasonable measures to establish the PEP's source of wealth and source of funds; and

iv. comply with Chapter 15 of the Rules.

THE CROWN MELBOURNE AND PERTH AML/CTF PROGRAMS

47. At all times on and from 1 March 2016, Crown Melbourne and Crown Perth could not commence to provide a designated service to a customer unless they:

a. each adopted and maintained a standard AML/CTF program; or

b. jointly adopted and maintained a joint AML/CTF program.

Particulars

Sections 81(1), 83, 84 and 85 of the Act.

Section 81(1) is a civil penalty provision: s81(2) of the Act.

Crown Melbourne – Standard AML/CTF Program

48. For the period from 1 March 2016 to 1 November 2020, Crown Melbourne purported to adopt and maintain a Part A standard AML/CTF program (the **Crown Melbourne Standard Part A Program**).

Particulars

The Crown Melbourne Standard Part A Program comprised:

Version 7.0 effective from 2 February 2016 to 19 January 2017, paragraphs 1 to 19;

Version 7.1 effective from 19 January 2017 to 27 November 2018, paragraphs 1 to 19;

Version 8 effective from 27 November 2018 to 1 November 2020, paragraphs 1 to 19.

The AML/CTF Act and AML/CTF Rules Compliance Guidelines (the **Crown Melbourne Guidelines**) were intended to provide information to employees of Crown Melbourne to assist with compliance with Crown Melbourne's AML/CTF Program and with the Act and Rules generally.

49. For the period from 1 March 2016 to 1 November 2020, Crown Melbourne purported to adopt and maintain a Part B standard AML/CTF program (the **Crown Melbourne Standard Part B Program**).

Particulars

The Crown Melbourne Standard Part B Program comprised:

Version 7.0 effective from 2 February 2016 to 19 January 2017, paragraphs 20 to 24;

Version 7.1 effective from 19 January 2017 to 27 November 2018, paragraphs 20 to 25;

Version 8 effective from 27 November 2018 to 1 November 2020, paragraphs 20 to 25.

Also see the Crown Melbourne Guidelines.

Crown Perth – Standard AML/CTF Program

50. For the period from 1 March 2016 to 1 November 2020, Crown Perth purported to adopt and maintain a Part A standard AML/CTF program (the **Crown Perth Standard Part A Program**).

Particulars

The Crown Perth Standard Part A Program comprised:

Version 14 effective from 28 April 2015 to 14 December 2016, paragraphs 1 to 17;

Version 15 effective from 14 December 2016 to 24 April 2017, paragraphs 1 to 17;

Version 16 effective from 24 April 2017 to 3 December 2018, paragraphs 1 to 17;

Version 17 effective from 3 December 2018 to 1 November 2020, paragraphs 1 to 17.

The 'Legal Services – AML Standard Operating Procedures' (**Crown Perth AML SOP**)'s purpose included to set out the operational procedures to be followed by the Legal Officer – AML (or designee) with respect to the Crown Perth AML/CTF Program.

51. For the period from 1 March 2016 to 1 November 2020, Crown Perth purported to adopt and maintain a Part B standard AML/CTF program (the **Crown Perth Standard Part B Program**).

Particulars

The Crown Perth Standard Part B Program comprised:

Version 14 effective from 28 April 2015 to 14 December 2016, paragraphs 18 to 20;

Version 15 effective from 14 December 2016 to 24 April 2017, paragraphs 18 to 20;

Version 16 effective from 24 April 2017 to 3 December 2018, paragraphs 18 to 20;

Version 17 effective from 3 December 2018 to 1 November 2020, paragraphs 18 to 20.

Also see the Crown Perth AML SOP.

Crown Melbourne's and Crown Perth's Joint AML/CTF Program

52. On and from 2 November 2020, Crown Melbourne and Crown Perth each purported to adopt and maintain a Part A joint AML/CTF program (the **Joint Part A Program**).

Particulars

The Joint Part A Program comprised:

Version 2 effective from 2 November 2020;

Version 3.0, approved on 21 December 2021, effective from 31 January 2022; and

Crown Resorts Limited Joint Anti-Money Laundering and Counter-Terrorism Financing Policy and Procedures, version 1.0, effective from 2 November 2020.

53. On and from 2 November 2020, Crown Melbourne and Crown Perth each purported to adopt and maintain a Part B joint AML/CTF program (the **Joint Part B Program**).

Particulars

The Joint Part B Program comprised:

Version 2 effective from 2 November 2020 to 10 August 2021;

Version 2.1 effective from 10 August 2021.

CROWN'S INFORMATION MANAGEMENT SYSTEMS

54. Crown Melbourne and Crown Perth had multiple information management systems to record information relevant to its customers and the provision of designated services.

55. At all times, **SYCO** was the information management system jointly used by Crown Melbourne and Crown Perth to:

a. record:

i. gaming activity;

ii. buy-in and pay-out or cash-out transactional data;

Particulars to ii.

The '**buy-in**' stage is when a customer purchases chips, tickets, or other CVIs in order to commence gambling.

The '**pay-out**' or '**cash-out**' stage is when a customer converts chips, tickets, other CVIs or gaming machine credits to money.

iii. cashier activity;

Particulars to iii.

The cashier is known as **the Cage**.

iv. customer account transactions; and

v. credit control functions.

b. interface with and capture data from other Crown systems, including:

   i. customer management systems such as **LUI** and **CC2**; and

   ii. the table games systems or **ATOM**;

c. generate manual reports for transaction monitoring purposes; and

d. generate xml files for bulk uploads to AUSTRAC of reports required under Part 3 of the Act.

56. LUI was introduced to Crown Perth and Crown Melbourne in November 2016, and was front-end customer management software, intended to be used to create customer profiles and update customer information.

57. CC2 was the back-end system to LUI, used to securely store the customer information Crown Melbourne and Crown Perth collected, including customer profiles, KYC information and ID scans.

58. At no time since November 2016 has LUI operated as a complete or accurate data source of information for Crown Melbourne and Crown Perth customers for the following reasons:

a. When LUI was introduced in November 2016, a process was commenced to generate consolidated unique identification numbers for customers across both Crown Melbourne and Crown Perth, starting with non-VIP customers.

b. It was not until October 2019 that LUI was used to register customers at Crown Melbourne and Crown Perth.

c. It was not until November 2019 that a duplicate check could be run across the entire customer base in LUI, including for VIP customers. Before that time, customer information from Crown Melbourne was not fully available to Crown Perth and vice versa.

d. Prior to November 2019, Crown Melbourne and Crown Perth could issue the same customer with more than one unique identification number.

e. The process to remediate legacy issues with multiple customer identification numbers is ongoing.

Particulars

See paragraphs 678 and 680.

59. At all times, data entered into LUI and CC2 needed to be synchronised with SYCO records in order for customer transactions to be linked to up-to-date customer profiles.

Particulars

Following LUI's implementation, a number of IT issues were identified, including with the automatic feeding of LUI information into the AUSTRAC reporting extracts generated from SYCO and with respect to duplicate customer accounts in SYCO, which increased the risk of inaccurate or out-of-date KYC information being retained on Crown Melbourne's and Crown Perth's systems and potentially reported to AUSTRAC. A working group was established in November 2017 to remediate these issues. A process of manual

checks was put in place to prevent IT issues from impacting AUSTRAC reporting.

60. The Security and Surveillance teams of Crown Melbourne used a system called **SEER**.

61. The main functions of SEER were to record:

    a. operational reporting by the Security and Surveillance teams;

    b. intelligence/event data against customer, such as entry of

        i. law enforcement requests,

        ii. lodgement of SMRs to AUSTRAC (as autogenerated and provided by SYCO);

    c. decisions to exclude or ban a customer in accordance with a process under State legislation; and

    d. decisions by Crown Melbourne to issue a withdrawal of the common law licence for a specific customer to enter the casino premises.

62. Crown Perth did not use SEER to record:

    a. the matters pleaded at paragraphs 61a to c; or

    b. decisions by Crown Perth to issue a notice revoking the common law licence for a specific customer to enter the casino premises.

63. From February 2020, **CURA** was available to Crown Melbourne as an AML/CTF customer intelligence database and central customer risk register.

64. Increasingly throughout 2020 and 2021 as the Crown Melbourne and Crown Perth AML team expanded, CURA was used to maintain a record of all customer ML/TF risk events, including:

    a. outcomes of the AML team's investigation processes, triggered by an Unusual Activity Report (**UAR**) or any other line of enquiry;

    b. updates where a non-investigation event occurred, such as classification of a customer as a PEP.

65. The financial crime team in Crown Perth started using CURA from 2013 and it was intended to be:

    a. a digital escalation system to document and manage incidents that presented risks to the organisation, including ML/TF risk;

    b. used to update the customer's risk profile where Crown Perth had identified a customer that matched ‘risk type’ in Appendix B to the Crown Perth Standard Part A Program.

66. The processes relating to data entry and the use of CURA by Crown Perth from 2013 were unclear. At no time prior to 2020/2021:

    a. was CURA used consistently by Crown Perth;

    b. did CURA provide Crown Perth with a full record of each customer’s ML/TF risk profile.

67. The risk-based procedures, systems and controls in Crown Melbourne’s and Crown Perth’s AML/CTF Programs were not capable, by design, of complying with the requirements of the Act and Rules because Crown Melbourne’s and Crown Perth’s information management systems did not enable these risk-based procedures, systems and controls to operate as intended.

Particulars

See paragraphs 120, 279, 455, 483, 613 to 628, 635, 675 to 683 and 706.

The procedures, systems and controls were not capable, by design, of operating in the manner described in the AML/CTF programs due to the deficiencies in information management systems. Consequently, Crown Melbourne's and Crown Perth's Standard Part A Programs did not establish risk-based systems and controls whose primary purpose was to identify, mitigate and manage ML/TF risk.

Section 84(2)(a) and (c) of the Act and rule 8.1.3 of the Rules.

THE AML/CTF PROGRAM CONTRAVENTIONS – SECTION 81

The Standard Programs

68. A reporting entity cannot adopt and maintain a standard AML/CTF program for the purposes of s81 of the Act unless it has adopted and maintained both a:

    a. standard Part A program; and

    b. standard Part B program.

Particulars

Section 84(1) of the Act.

The Standard Part A Programs

69. A reporting entity cannot adopt and maintain a standard Part A program for the purposes s81 of the Act unless the Part A program complies with the requirements of:

    a. section 84(2)(a) of the Act;

    b. section 84(2)(c) of the Act; and

    c. rules made under s84(2)(c) of the Act, including Chapters 8 and 15 of the Rules.

70. From 1 March 2016 to 1 November 2020, the Crown Melbourne and Crown Perth Standard Part A Programs (the **Standard Part A Programs**) did not meet the requirements of s84(2) of the Act and Chapters 8 and 15 of the Rules because the Standard Part A Programs did not:

    a. have the **primary purpose of identifying, mitigating and managing the ML/TF risks** that Crown Melbourne and Crown Perth reasonably faced and did not comply with the requirements of the Rules.

Particulars

Sections 84(2)(a) and (c) of the Act and rules 8.1.3. 8.1.4, 8.1.5, 8.4. 8.6 and 8.7 of the Rules.

See paragraphs 86 to 583.

    b. include a **transaction monitoring program** that complied with the requirements of the Rules.

Particulars

Section 84(2)(c) of the Act and rules 8.1.3, 8.1.4, and 15.4 to 15.7 of the Rules.

See paragraphs 584 to 651.

c. include an **enhanced customer due diligence program** that complied with the requirements of the Rules.

Particulars

Section 84(2)(c) of the Act and rules 1.2.1, 8.1.3, 8.1.4 and 15.8 to 15.11 of the Rules.

See paragraphs 652 to 683.

d. include systems and controls designed to ensure Crown Melbourne and Crown Perth complied with the **reporting requirements under Part 3 of the Act**.

Particulars

Rule 8.9.1(2) of the Rules, made for the purposes of s 84(2)(c) of the Act.

See paragraphs 684 to 691.

71. By reason of the matters pleaded in paragraphs 69 and 70, Crown Melbourne and Crown Perth did not adopt and maintain a standard Part A program for the purposes s81 of the Act from 1 March 2016 to 1 November 2020.

72. By reason of the matters pleaded in paragraphs 6, 7, 68 and 71, Crown Melbourne and Crown Perth commenced to provide designated services from 1 March 2016 to 1 November 2020 in contravention of s81(1) of the Act.

73. By reason of the matters pleaded in paragraph 72, Crown Melbourne and Crown Perth each contravened s81(1) of the Act on each occasion that they provided a designated service from 1 March 2016 to 1 November 2020.

Particulars

Section 81(1) of the Act is a civil penalty provision: s81(2) of the Act.

The Standard Part B Programs

74. A reporting entity cannot adopt and maintain a standard Part B program for the purposes s81 of the Act unless the Part B complies with the requirements of:

a. section 84(3)(a) of the Act;

b. section 84(3)(b) of the Act; and

c. rules made under s84(3)(b) of the Act, including Chapter 4 of the Rules.

75. From 1 March 2016 to 1 November 2020, the Crown Melbourne and Crown Perth Standard Part B Programs (the **Standard Part B Programs**) did not comply with the requirements of s 84(3) of the Act because they did not:

a. set out the ACIPs for the purposes of the application of the Act to all customers of Crown Melbourne and Crown Perth: s84(3)(a); and

b. comply with requirements of Chapter 4 of the Rules made under s84(3)(b) of the Act.

Particulars

Chapter 10 and rule 14.4 of the Rules made under s39 of the Act.

See paragraphs 693 to 708.

76. By reason of the matters pleaded in paragraph 75, Crown Melbourne and Crown Perth did not adopt and maintain a standard Part B program for the purposes s81 of the Act from 1 March 2016 to 1 November 2020.

77. By reason of the matters pleaded in paragraphs 6, 7, 68 and 76 Crown Melbourne and Crown Perth commenced to provide designated services from 1 March 2016 to 1 November 2020 in contravention of s81(1) of the Act.

78. By reason of the matters pleaded in paragraph 77, Crown Melbourne and Crown Perth each contravened s 81(1) of the Act on each occasion that they provided a designated service from 1 March 2016 to 1 November 2020.

Particulars

Section 81(1) of the Act is a civil penalty provision: s81(2) of the Act.

The Joint Program - Part A and Part B

79. A reporting entity cannot adopt and maintain a joint AML/CTF program for the purposes of s81 of the Act unless it has adopted and maintained both a:

a. joint Part A program that meets the requirements of s85(2) of the Act and Chapters 9 and 15 of the Rules (made under s85(2)(c)); and

b. joint Part B program that meets the requirements of s85(3) of the Act and Chapter 4 of the Rules (made under s85(3)(b)).

Particulars

Section 85(1) of the Act.

80. On and from 2 November 2020, Crown Melbourne and Crown Perth did not adopt and maintain a joint Part A program that met the requirements of the Act and Rules, by reason of the matters pleaded in paragraphs 709 to 724.

81. By reason of the matters pleaded in paragraph 6, 7, 79 and 80, Crown Melbourne and Crown Perth commenced to provide designated services on and from 2 November 2020 in contravention of s 81(1) of the Act.

82. By reason of the matters pleaded in paragraph 81, Crown Melbourne and Crown Perth each contravened s 81(1) of the Act on each occasion that they provided a designated service on and from 2 November 2020.

Particulars

Section 81(1) of the Act is a civil penalty provision: s81(2) of the Act.

83. On and from 2 November 2020, Crown Melbourne and Crown Perth did not adopt and maintain a joint Part B program that met the requirements of the Act and Rules, by reason of the matters pleaded in paragraphs 726 to 727.

84. By reason of the matters pleaded in paragraph 6, 7, 79, and 83, Crown Melbourne and Crown Perth commenced to provide designated services on and from 2 November 2020 in contravention of s81(1) of the Act.

85. By reason of the matters pleaded in paragraph 84, Crown Melbourne and Crown Perth each contravened s81(1) of the Act on each occasion that they provided a designated service on and from 2 November 2020.

Particulars

Section 81(1) of the Act is a civil penalty provision: s81(2) of the Act.

THE STANDARD AML/CTF PROGRAM CONTRAVENTIONS – s81

The primary purpose of identifying, mitigating and managing ML/TF risks reasonably faced

86. From 1 March 2016 to 1 November 2020, the Standard Part A Programs did not:

a. have the primary purpose of identifying, mitigating and managing the ML/TF risks that each reporting entity reasonably faced with respect to designated services for the purposes of s84(2)(a); and

b. comply with the requirements specified in the Rules for the purposes of s84(2)(c)

for the reasons pleaded at paragraphs 87 to 90 below.

87. The Standard Part A Programs did not include an appropriate **risk methodology** that was capable of appropriately identifying and assessing the ML/TF risks of its designated services for the reasons pleaded at paragraphs 91 to 99.

88. The Standard Part A Programs were not **aligned to the ML/TF risks reasonably faced** by Crown Melbourne and Crown Perth with respect to the provision of designated services for the reasons pleaded at paragraphs 100 to 136.

89. The Standard Part A Programs did not include or establish an **appropriate approval and oversight framework** that was capable by design of identifying, mitigating and managing the ML/TF risks reasonably faced by Crown Melbourne and Crown Perth and of meeting the requirements of the Rules for the reasons pleaded at paragraphs 137 to 201.

90. The Standard Part A Programs did not include **appropriate risk-based systems and controls** that were capable by design of identifying, mitigating and managing the ML/TF risks reasonably faced by Crown Melbourne and Crown Perth with respect to:

a. **Gaming accounts**, including:

i. Deposit accounts (**DAB accounts**) and safekeeping accounts for the reasons pleaded at paragraphs 208 to 254;

ii. Card Play Extra accounts for the reasons pleaded at paragraphs 208 and 255 to 279;

b. **Loans and transactions relating to loans**, including:

i. Credit facilities for the reasons pleaded at paragraphs 280 to 302, and 395;

ii. Cheque cashing facilities (**CCFs**) for the reasons pleaded at paragraphs 280, 303 to 331, and 395;

iii. Overseas deposit services for the reasons pleaded at paragraphs 280 and 332 to 395.

c. **Remittance services** for the reasons pleaded at paragraphs 396 to 423.

d. The **exchange of money for casino value instruments such as chips and tickets (and vice-versa)** for the reasons pleaded at paragraphs 424 to 428.

e. **Table games and electronic gaming machines** for the reasons pleaded at paragraphs 429 to 435.

f. **Foreign currency exchange**, for the reasons pleaded at paragraphs 436 to 442.

g. **Designated services provided in foreign currency**, for the reasons pleaded at paragraphs 443 to 447.

h. **Designated services provided in cash** for the reasons pleaded at paragraphs 448 to 455.

i. **Designated services involving third party transactions** for the reasons pleaded at paragraphs 456 to 463.

j. **Designated services provided through junket channels** for the reasons pleaded at paragraphs 464 to 583.

Risk methodologies

91. A standard Part A program will not be capable, by design, of identifying, mitigating and managing ML/TF risks if it does not include an appropriate risk methodology to identify and assess the ML/TF risks of the designated services provided by the reporting entity.

Particulars

Sections 84(2)(a) and (c) of the Act and rules 8.1.3, 8.1.4 and 8.1.5 of the Rules.

92. From 1 March 2016 to 1 November 2020, the Standard Part A Programs did not include or incorporate an appropriate risk methodology that was capable of appropriately identifying and assessing the ML/TF risks of its designated services for the reasons pleaded at paragraphs 93 to 99 below.

Particulars

Sections 84(2)(a) and (c) of the Act and rules 8.1.3, 8.1.4 and 8.1.5 of the Rules.

93. The Standard Part A Programs did not include or incorporate a methodology to appropriately assess the inherent ML/TF risks with respect to designated services.

Particulars

The Standard Part A Programs did not include a methodology to measure the likelihood and impact of inherent ML/TF risks.

Nor did the Programs include a methodology that covered all relevant inherent risks and associated risk attributes reasonably faced by Crown Melbourne and Crown Perth with respect to each designated service.

The Standard Part A Programs did not include a methodology that had regard to the nature, size and complexity of the Crown Melbourne and Crown Perth businesses.

Rules 8.1.3 and 8.1.4 of the Rules.

See paragraphs 12 to 26 above.

94. The Standard Part A Programs did not include or incorporate a methodology to appropriately consider the ML/TF risks posed by the types of designated services provided by Crown Melbourne and Crown Perth.

Particulars

There was no methodology that appropriately applied to all designated service types provided by Crown Melbourne and Crown Perth, including both table 1, s6 financial services and table 3, s6 gaming services.

Rule 8.1.4(2) of the Rules.

95. The Standard Part A Programs did not include or incorporate a methodology to appropriately consider the risk factor of channel in assessing the ML/TF risks posed by designated services.

Particulars

Rule 8.1.4(3) of the Rules.

96. The Standard Part A Programs did not include or incorporate a methodology to appropriately consider the risk factor of foreign jurisdictions in assessing the ML/TF risks posed by designated services.

Particulars

Rule 8.1.4(4) of the Rules.

97. The Standard Part A Programs did not include or incorporate a methodology to appropriately consider the ML/TF risks posed by customer types receiving designated services:

Particulars

Rule 8.1.4(1) of the Rules.

a. The Standard Part A Programs did not appropriately identify and define the categories of customers that were not low risk, including international VIP and junket channel customers.

Particulars

Annexure G of the Crown Melbourne Standard Part A Program.

Appendix B of the Crown Perth Standard Part A Program.

See paragraphs 117 to 126.

b. The Standard Part A Programs did not include appropriate criteria or risk parameters for categorising customer types who were not low risk.

Particulars

Annexure G of the Crown Melbourne Standard Part A Program.

Appendix B of the Crown Perth Standard Part A Program.

98. The Standard Part A Programs did not include or incorporate a methodology to appropriately assess the ML/TF risks reasonably faced by Crown Melbourne and Crown Perth with respect to complex designated service chains, having regard to the nature, size and complexity of their business including that:

a. during the course of a visit to the casino, customer funds could be moved through cash, gaming chips and gaming accounts (table 3, s6 services), and transferred to or from third parties, another casino, or a domestic or foreign bank (items 31 and 32, table 1, s6 and item 13, table 3 s6 services);

b. the designated services provided to customers could involve long and complex transactional value chains ranging from receipt of funds, account management, gaming activities and outward disbursement of funds; and

c. these transactional chains involved different channels and jurisdictions.

Particulars

Rules 8.1.3 and 8.1.4 of the Rules.

99. The Standard Part A Programs did not include a methodology to assess the residual ML/TF risks of designated services, once risk-based controls had been applied.

Particulars

Rules 8.1.3 and 8.1.4 of the Rules.

Alignment of the Standard Part A Programs to ML/TF risk

100. Once a reporting entity identifies the ML/TF risks it reasonably faces, and carries out an assessment of those risks in accordance with an appropriate ML/TF risk methodology, the reporting entity must align its Part A Program to those risks as assessed.

Particulars

Sections 84(2)(a) and (c) and rules 8.1.3 and 8.1.4 of the Rules.

101. In aligning a Part A Program to the ML/TF risks reasonably faced, a reporting entity must have regard to:

a. the nature, size and complexity of its business; and

b. the type of ML/TF risks it reasonably faces.

Particulars

Rule 8.1.3 of the Rules.

102. When having regard to the ML/TF risk it reasonably faces, a reporting entity must have regard to the risk factors of:

a. designated services;

b. customers;

c. channel; and

d. foreign jurisdictions.

Particulars

Rule 8.1.4 of the Rules.

103. The ML/TF risks reasonably faced by Crown Melbourne and Crown Perth with respect to designated services are also dynamic.

104. A reporting entity must review and update ML/TF risk assessments, at intervals that are appropriate having regard to the nature, size and complexity of its business.

Particulars

Rules 8.1.3 and 8.1.5 of the Rules.

105. For the reasons pleaded in paragraphs 106 to 128, at no time were the Standard Part A Programs aligned to the ML/TF risks reasonably faced by Crown Melbourne and Crown Perth having regard to the requirements pleaded at paragraphs 100 to 104.

The Risk Registers

106. The Standard Part A Programs included a ML/TF Risk Register (the **Risk Register**).

Particulars

The Crown Melbourne Standard Part A Programs included a Risk Register at Annexure E, Appendix 1.

The Crown Perth Standard Part A Programs included a Risk Register at Appendix E.

107. The Risk Registers purported to record:

a. the ML/TF risks reasonably faced by Crown Melbourne and Crown Perth; and

b. the systems and controls intended to mitigate and manage those ML/TF risks.

108. The Risk Registers did not clearly articulate a number of ML/TF risks that Crown Melbourne and Crown Perth might reasonably have faced with respect to the provision of designated services, including:

a. risks with respect to customer types, including PEPs, high spenders, VIPs, casual customers and customers the subject of law enforcement inquiries;

b. risks with respect to different product or designated service type, including accounts/account activities; and risks associated with designated services being used to move proceeds of crime;

c. channel risk, including on face-to-face channels, junket channels, private gaming rooms and 'Crown Patron accounts' (as defined at paragraph 225);

d. jurisdiction risk, including geographical or country risk; and

e. ML/TF typologies and vulnerabilities (as defined at paragraph 24), including but not limited to:

i. cuckoo smurfing;

ii. the involvement of third parties in relation to customer transactions;

iii. offsetting;

iv. customers attempting to deposit front money or make payments using complex means;

v. customer requests for transfers to and from other casinos;

vi. dramatic increases in gaming activity, including escalating rates of high turnover or high losses;

vii. money parked in accounts;

viii. misuse of CVIs;

ix. intentional losing or collusion; and

x. loan sharking.

Particulars

By no later than June 2018, the Chief Legal Officer of Crown Resorts, who was also the AMLCO for both Crown Melbourne and Crown Perth, was advised by the Group General Manager AML that the Crown Melbourne AML/CTF Program had not been updated for some time; and that key ML/TF risks were not on the Risk Register and did not form part of the transaction monitoring program.

109. The risks included in the Risk Register had not been assessed in accordance with an appropriate risk methodology.

Particulars

See paragraph 92 above.

110. The Risk Register did not include appropriate risk-based controls that, by design, were capable of identifying, mitigating and managing the ML/TF risks reasonably faced by Crown Melbourne.

111. The controls listed in the Risk Register did not provide a basis for Crown Melbourne and Crown Perth to determine that residual risk was low.

The ML/TF risk factors

The ML/TF risks factors - designated services

112. The risk-based systems and controls in the Standard Part A Programs were not aligned to the ML/TF risks reasonably faced by Crown Melbourne and Crown Perth with respect to each of the designated services they provided item tables 1 and 3, s6 of the Act.

113. At no time did Crown Melbourne and Crown Perth appropriately identify and asses the ML/TF risks of designated services according to an appropriate methodology, as pleaded at paragraph 92 above.

114. At no time did the Standard Part A Programs include appropriate risk-based controls to identify, mitigate and manage the ML/TF risks of designated services, as pleaded at paragraphs 202 to 583 below.

Particulars

Rule 8.1.4(2) of the Rules.

The ML/TF risk factors - customers

115. The risk-based procedures, systems and controls in the Standard Part A Programs were not aligned to the ML/TF risks reasonably faced by Crown Melbourne and Crown Perth with respect to customers, for the reasons pleaded at paragraphs 116 to 126 below.

Particulars

Rules 8.1.4(1), 8.1.5(1), 15.2 and 15.3 of the Rules.

116. For the reasons pleaded at paragraph 92, the Standard Part A Programs did not establish a framework that enabled Crown Melbourne or Crown Perth to appropriately categorise and rate the risks posed by different types of customers.

117. The Standard Part A Programs stated that all Crown Melbourne and Crown Perth customers were automatically rated low ML/TF risk by default (the **default rating**), unless the Programs or a decision made under them required otherwise.

Particulars

Clause 13 of the Standard Part A Programs.

118. At all times, the Crown Melbourne Standard Part A Programs also required the following types of customers to have an automatic high risk rating:

a. customers known to have engaged in ML/TF; or

b. customers known to be a foreign PEP; or

c. a company.

Particulars

Annexure G of the Crown Melbourne Standard Part A Programs.

119. At all times, the Crown Perth Standard Part A Programs also required customers known to have engaged in ML/TF to have an automatic high risk rating.

Particulars

Appendix B of the Crown Perth Standard Part A Programs.

120. The Standard Part A Programs did not include appropriate procedures to trigger an assessment of a customer's risk rating to determine if they were not low risk by default.

a. The Standard Part A Programs did not include procedures to identify customers who were required to be rated automatically as high risk.

b. The Crown Melbourne Cash Transactions Reporting Manager (**CTRM)** in Melbourne or the AMLCO/Ratings Officer in Crown Perth, was primarily responsible for determining whether to conduct assessments of customer risk ratings.

c. There were no procedures to consistently escalate potentially higher risk customers to the CTRM or AMLCO/Ratings Officer for assessment.

d. Prior to 1 December 2018, Crown Melbourne screened all active customers with a significant or high risk rating through World-Check three times a week. An active customer was a customer that had activity noted against their account or Crown Rewards membership at a Crown entity within the previous 30 days. This process, by definition, was not applied to customers who were considered low risk by default.

e. Prior to 1 December 2018, Crown Perth completed a report from FicroSoft data search system for any person listed in World-Check as a terrorist, criminal or PEP. However, the review of those reports was manual.

f. From 1 December 2018, Crown Melbourne and Crown Perth ran a daily screen of all new customers, any existing customers who had updated their KYC information and all active customers through Dow Jones Risk and Compliance database. This was a consolidated list which was run across customers of both Crown Melbourne and Crown Perth.

g. The Crown Perth Standard Part A Program also required a World-Check on applications for deposit and credit facilities, on individual players on a junket program, customers on a premium program, or customers who were recorded as incoming international business to the Pearl Room.

h. At all times, the CTRM or Financial Crime team (in Melbourne) or the Legal Officer, AML was required to manually review screening results to identify customers who may have required an active risk assessment. This review process was not adequately resourced and was not appropriately risk based. Screening was conducted against customer data on SYCO. Customer information entered on SYCO was not always reliable.

Particulars

See paragraphs 613 to 625.

i. The Standard Part A Programs also provided for other daily, weekly and monthly systems generated reports. For the reasons pleaded at paragraphs 603 to 609, these processes were not capable of consistently identifying customers who were not low risk.

j. Many of the triggers in the Crown Melbourne Standard Part A Programs for rating a customer moderate risk or above relied on identifying transactional activity within certain parameters. The transaction monitoring program was not capable by design of identifying that activity.

Particulars

See paragraph 594 below.

For the period from July 2020 to 30 June 2021, only 4% of carded Crown Melbourne and Crown Perth customers had been assigned a proactive risk rating, with the balance being considered 'low risk' by default.

Carded play was play recorded against a Crown Rewards account, by swiping the customer's Crown Rewards card at the time of entering into the game.

121. The Standard Part A Programs did not include or incorporate appropriate guidance or criteria for assessing customers who may not have been low risk:

a. The decision to rate a customer above the default of low risk was at the discretion of the CTRM at Crown Melbourne.

b. The decision to rate a customer above the default of low risk was at the discretion of the AMLCO and/or the AML/CTF Compliance Officer, or from 2018 the Ratings Officers at Crown Perth.

c. The Standard Part A Programs did not include any risk parameters against which to assess customer risk.

Particulars

By no later than June 2018, the Chief Legal Officer of Crown Resorts, who was also the AMLCO for both Crown Melbourne and Crown Perth, was advised by the Group General Manager AML (Crown Melbourne) that the assessment and analysis of customer risk by Crown Melbourne was arbitrary and not subject to any concrete risk parameters.

d. The Standard Part A Programs did not include any guidance or criteria on assessing the ML/TF risks of customers with respect to table 1, s6 financial services, including with respect to loans and remittance services.

e. The credit risk team carried out assessments of the credit risks posed by some international players and junkets visiting Crown Melbourne and Crown Perth. These credit risk assessments were not subject to any guidance or criteria relevant to ML/TF risks.

122. At no time did the Standard Part A Programs include or incorporate appropriate risk-based procedures to collect and analyse appropriate KYC information for the purposes of assessing a customer's risk, including with respect to source of wealth or source of funds.

a. Whilst Crown Melbourne and Crown Perth requested occupation information from customers in accordance with the Standard Part A Programs, it was optional for the customer to provide this.

Particulars

Annexure G of the Crown Melbourne Standard Part A Program.

Appendix F of the Crown Perth Standard Part A Program.

b. In the absence of a risk-based requirement in the Standard Part A Programs to obtain and assess information about source of wealth/funds (such as occupation), Crown Melbourne and Crown Perth were unable to understand the risk posed by certain customers.

Particulars

See the definition of 'KYC Information' in rule 1.2.1 of the Rules in relation to customers who are individuals.

Source of wealth and source of funds information was not necessarily required from all customers. However, there were higher ML/TF risks related to source of wealth and source of funds for international VIP customers and high rollers, among others.

c. The Standard Part A Programs did not include appropriate risk-based processes to collect or verify further KYC information relating to the beneficial ownership of funds or the beneficiaries of transactions being facilitated, including the destination of funds.

Particulars

Rules 8.1.5, 15.2 and 15.3; and paragraphs (l) and (m) of the definition of KYC information in rule 1.2.1 of the Rules.

123. The Standard Part A Programs did not include or incorporate any assurance processes relating to the methodology to assign risk ratings to customers.

124. The Standard Part A Programs did not include appropriate risk-based systems and controls to mitigate and manage the ML/TF risks of customers who had been assessed as high risk.

Particulars

See paragraphs 652 to 656.

125. At no time did the Standard Part A Programs establish appropriate information management systems with respect to customer risk assessments.

a. At Crown Melbourne, the record of a customer's risk assessment was stored in local drives and was not available to front line staff for the purposes of the Part A procedures, systems and controls.

b. When Crown Perth identified risk information that matched a 'risk type' in Appendix B of the Standard Part A Programs, it was required to enter this information in the Risk Register. The Risk Register was an excel spreadsheet, which was uploaded to CURA. CURA was not updated consistently because Crown Perth did not keep records each time it obtained risk information.

Particulars

Clause 13 and Appendix B in each version of the Crown Perth Standard Part A Program.

See paragraph 682.

126. The Standard Part A Programs did not include appropriate risk-based controls to identify customers who presented ML/TF risks outside of risk appetite.

Particulars

Sections 84(2)(a) and 84(2)(c) of the Act and Parts 8 and 15 of the Rules.

The ML/TF risk factors - channel

127. The risk-based procedures, systems and controls in the Standard Part A Programs were not aligned to the ML/TF risks reasonably faced by Crown Melbourne and Crown Perth having regard to the channels through which designated services were delivered for the following reasons:

a. The Risk Register did not adequately or appropriately address channel risk.

b. Crown Patron accounts (see paragraph 225 below) were not recognised by the Standard Part A Programs as a channel through which designated services were provided and the ML/TF risks of this channel were therefore not assessed.

c. The Hotel Credit Transactions channel (see paragraph 244 below) was not recognised by the Standard Part A Programs as a channel through which designated services were provided and the ML/TF risks of this channel were therefore not assessed.

d. The Standard Part A Programs did not appropriately recognise that some item 31 and 32, table 1, s6 designated services (remittance services) are not provided face-to-face, including those provided through the Crown Patron account channel above.

e. The Standard Part A Programs did not appropriately recognise that some item 13 table 3, s6 designated services (account transactions) are not provided face-to-face, including those provided through the Crown Patron account channel above.

f. The Standard Part A Programs did not appropriately recognise that some item 7 table 1, s6 designated services (credit facilities and cheque cashing facilities) are not provided face-to-face.

g. The Standard Part A Programs did not include appropriate risk-based systems and controls that were aligned to the ML/TF risks of providing designated services through junket channels, for the reasons pleaded at paragraphs 464 to 583.

h. As a result of the matters pleaded at sub-paragraphs a to g, the Standard Part A Programs did not include risk-based systems and controls that applied to and were aligned to each of these channel risks.

Particulars

Rule 8.1.4(3) of the Rules.

The ML/TF risk factors - jurisdiction

128. The risk-based procedures, systems and controls in the Standard Part A Programs were not aligned to the ML/TF risks reasonably faced by Crown Melbourne and Crown Perth with respect to designated services having regard to foreign jurisdictions for the following reasons:

a. The Risk Register did not adequately or appropriately address jurisdiction risk.

b. The Standard Part A Programs did not identify the foreign jurisdictions that Crown Melbourne and Crown Perth dealt with.

c. The Crown Melbourne Standard Part A Program, rated all foreign jurisdictions 'low risk' by default, with the following exceptions:

i. Iran and North Korea were 'high risk'.

ii. From 1 December 2014, countries on the Department of Foreign Affairs and Trade sanctions list were 'high risk'.

iii. From 23 November 2018, FATF high risk and non-cooperative jurisdictions and ML/TF risk environments identified by the Attorney-General's Department were 'high risk'.

d. Appendix E in Crown Perth's Standard Part A Program required that jurisdiction be considered (once known) by utilising recognised lists published by the relevant Government authorities, but there were no procedures setting out when a consideration of jurisdiction would occur for the purposes of Part A.

e. Neither of the Standard Part A Programs included any risk-based procedures, systems or controls that applied to high risk jurisdictions.

f. The Standard Part A Programs did not identify how jurisdictional risks were factored into customer risk profiles.

g. The CTRM (Crown Melbourne) or AMLCO (Crown Perth) had discretion to determine how jurisdiction impacted customer risk. This was not capable of consistent application.

h. The Standard Part A Programs did not identify how jurisdictional risks were factored into the assessment of the ML/TF risks of designated services and channels.

Particulars

Rule 8.1.4(4) of the Rules.

Changing or emerging ML/TF risks - reviewing and updating ML/TF risk assessments and controls

129. At no time did the Standard Part A Programs include appropriate risk-based systems and controls to identify significant changes in ML/TF risks and to recognise such changes for the purposes of the Standard Part A and Standard Part B Programs for the reasons pleaded at paragraphs 130 to 136.

Particulars

Sections 84(2)(a) and 84(2)(c) of the Act and rules 8.1.5(3) and 8.1.5(4) of the Rules.

130. By reason of the matters pleaded at paragraphs 108 to 111 above, at all times the Risk Register was fundamentally deficient and did not include key ML/TF risks reasonably faced.

131. By reason of the matters pleaded in paragraph 130, the annual reviews of the Risk Register on their own were not capable of identifying significant changes in ML/TF risks and recognising such changes for the purposes of the Standard Part A and Standard Part B Programs.

Particulars

The requirement for an annual review of the Risk Register is set out in Annexure E of the Crown Melbourne Standard Part A Program and Appendix E of the Crown Perth Standard Part A Program.

Each of the reviews of the Risk Register conducted from 2016 to 1 November 2020 failed to recognise and address the fundamental deficiencies in the Risk Register, as pleaded at paragraphs 108 to 111 above.

132. As the Standard Part A Programs did not include an appropriate risk methodology, ML/TF risks were not capable of being consistently assessed and re-assessed over time.

Particulars

See paragraphs 91 to 99 above.

133. The Standard Part A Programs did not include risk-based procedures for Crown Melbourne and Crown Perth to identify and assess trends arising from or disclosed by:

a. usage of designated services or channels;

b. transaction monitoring;

c. suspicious matter reporting;

d. internal financial crime reporting;

e. information from AUSTRAC and law enforcement; and

f. the external risk environment.

134. The Standard Part A Programs did not include appropriate risk-based procedures to escalate emerging trends to senior management.

135. The Standard Part A Programs did not provide procedures for appropriate Board and senior management oversight of the Risk Register for the purposes of identifying and recognising significant changes in risk.

Particulars

See paragraphs 137 to 201.

136. At no time did the Standard Part A Programs include appropriate risk-based systems and controls to identify, mitigate and manage any ML/TF risks arising from:

a. all new designated services prior to introducing them:

i. The Standard Part A Programs purported to provide for a procedure for the assessment of the risk of new designated services.

Particulars to ai.

Clause 8 and Annexure J of the Crown Melbourne Standard Part A Program.

Clause 8 and Appendix H of the Crown Perth Standard Part A Program.

ii. The assessments undertaken by Crown Melbourne and Crown Perth were not appropriately documented, were not conducted in accordance with any ML/TF risk methodology, were not directed towards ML/TF risks and did not fully address the matters specified by rule 8.1.5(5) of the Rules.

iii. From August 2017, Crown Melbourne could assess a new designated service using the AML/CTF Approval Form and, from April 2018, using the Gaming Initiatives Form.

iv. From March 2016, Crown Perth could assess a new designated service using the AML/CTF Approval Form and, from April 2018, using the Gaming Initiatives Form on an ad hoc basis.

v. There was no guidance on the factors to consider when completing these forms; nor was it mandatory to use the forms.

vi. Crown Melbourne did not document the risk assessments for proposed new games, services or procedures undertaken in the period prior to May 2018.

b. all new methods of designated service delivery (channel) prior to adopting them; and

i. The Standard Part A Programs contained no risk-based systems and controls to identify, mitigate and manage any ML/TF risks arising from new methods of designated service delivery (channel) prior to adopting them.

ii. The processes that were used were not appropriately documented, were not conducted in accordance with any ML/TF risk methodology, were not directed

towards ML/TF risks and did not fully address the matters specified by rule 8.1.5(5) of the Rules.

iii. Significantly, there were no procedures in place to assess the ML/TF risks of the Suncity account channel (as defined in paragraph 423 below) prior to its adoption.

c. all new or developing technologies for the provision of designated services prior to introducing them.

i. The processes that were used were not appropriately documented, were not conducted in accordance with any ML/TF risk methodology, were not directed towards ML/TF risks and did not fully address the matters specified by rule 8.1.5(5) of the Rules.

Particulars

Sections 84(2)(a) and 84(2)(c) of the Act and rule 8.1.5(5) of the Rules.

Approval and oversight of the Standard Part A Programs

Approval of the Standard Part A Programs

Crown Melbourne

137. At all times, Crown Melbourne was the reporting entity providing designated services through the Crown Melbourne casino.

138. At all times,

a. the Board of Crown Melbourne (the **Crown Melbourne Board**); and

b. Crown Melbourne senior management

were each required to approve the Crown Melbourne Standard Part A Program.

Particulars

Sections 84(2)(a) and (c) of the Act and rule 8.4.1 of the Rules.

139. The Crown Melbourne Standard Part A Program provided that either the Crown Melbourne Chief Executive Officer (**CEO**) or Australian Resorts CEO must approve any amendment to the Crown Melbourne Standard Part A Program.

Particulars

Clause 3 of the Crown Melbourne Standard Part A Program.

Annexure A of the Crown Melbourne Standard Part A Programs note a delegation by the Crown Melbourne Board to the CEO to approve amendments to the program.

140. **Australian Resorts** was a term used to describe Crown Resorts' Australian based resorts and casinos, including Crown Melbourne and Crown Perth.

141. At all times from 1 March 2016 to December 2020, the Australian Resorts CEO was:

a. a single role that combined the roles of both CEO for Crown Melbourne and CEO for Crown Perth; and

b. a role that was occupied by the same person.

142. At no time did the Crown Melbourne Standard Part A Program require both the Crown Melbourne Board and Crown Melbourne senior management to approve the Crown Melbourne Standard Part A Program.

143. In accordance with the specification in Crown Melbourne's Standard Part A Program referred to in paragraph 139 above, version 8 of the Crown Melbourne Standard Part A Program was approved by the Australian Resorts/Crown Melbourne CEO.

144. In contravention of rule 8.4.1 of the Rules and s 84(2)(c) of the Act, version 8 of the Crown Melbourne Standard Part A Program was not approved by the Crown Melbourne Board.

Crown Perth

145. At all times, Burswood Nominees Limited was the reporting entity providing designated services through the Crown Perth casino.

146. At all times:

a. the Board of Burswood Nominees Limited (the **Crown Perth Board**); and

b. Crown Perth senior management

were each required to approve the Crown Perth Standard Part A Program.

Particulars

Sections 84(2)(a) and (c) of the Act and rule 8.4.1 of the Rules.

147. The Crown Perth Standard Part A Program provided that the Crown Perth CEO and/or Board of Directors must approve any substantive amendment to the Crown Perth Standard Part A Program.

Particulars

Clause 3 of the Crown Perth Standard Part A Program.

148. At no time did the Crown Perth Standard Part A Program require both the Crown Perth Board and Crown Perth senior management to approve the program.

149. Prior to November 2020, the Australian Resorts/Crown Perth CEO approved each version of the Crown Perth Standard Part A Program.

150. In contravention of rule 8.4.1 of the Rules and s 84(2)(c) of the Act, the Crown Perth Board did not approve any version of the Crown Perth Standard Part A Program from 1 March 2016 until November 2020.

Oversight of the Standard Part A Programs

151. The Crown Melbourne Standard Part A Program was required to be subject to the ongoing oversight of Crown Melbourne's Board and senior management.

Particulars

Sections 84(2)(a) and (c) of the Act and rule 8.4.1 of the Rules.

152. The Crown Perth Standard Part A Program was required to be subject to the ongoing oversight of Crown Perth's Board and senior management.

Particulars

Sections 84(2)(a) and (c) of the Act and rule 8.4.1 of the Rules.

See paragraphs 189 to 192 below.

153. The oversight required of the Board and senior management of Crown Melbourne and Crown Perth included oversight of how, and the extent to which, the Standard Part A Programs were achieving the primary purpose of identifying, mitigating and managing ML/TF risk.

Particulars

Sections 84(2)(a) and (c) of the Act and rule 8.4.1 of the Rules.

154. In the absence of an appropriate oversight framework, a Part A program will not be capable, by design, of:

a. identifying, mitigating and managing the ML/TF risks reasonably faced by a reporting entity; and

b. being subject to the ongoing oversight of the reporting entity's Board and senior management.

155. A reporting entity of the nature, size and complexity of Crown Melbourne and Crown Perth will not be in a position to have an appropriate oversight framework, for the purposes pleaded at paragraph 154, unless their Part A Program has established an appropriate framework for the Board and senior management to:

a. determine and set the reporting entity's ML/TF risk appetite;

b. set controls to ensure designated services are provided to customers consistent with that ML/TF risk appetite;

c. appropriately monitor management's performance against an appropriate ML/TF risk management framework, including risk appetite;

d. ensure the Board receives and reviews management reports about new and emerging sources of ML/TF risk and about the measures management are taking to deal with those risks;

e. establish appropriate ML/TF risk management capability frameworks, including with respect to:

i. roles and accountabilities;

ii. operational procedures;

iii. reporting lines;

iv. escalation procedures;

v. assurance and review; and

vi. information management.

Particulars

Sections 81, 84(2)(a) and 84(2)(c) of the Act, rules 8.1.3, 8.1.5(4) and Part 8.4 of the Rules.

156. Each of the features alleged at paragraphs 155(a) to (e) was absent from the Standard Part A Programs for all or most of the period from 1 March 2016 to 1 November 2020.

Particulars

Paragraphs 157 to 201 below.

Crown Resorts

157. Prior to mid-2020:

a. Neither the Crown Resorts Board nor Crown Resorts' Risk Management Committee (**RMC**) received regular dedicated reports or updates that addressed AML/CTF matters specific to Crown Melbourne or Crown Perth;

b. AML/CTF matters relating to Crown Melbourne and Crown Perth were reported to the Crown Resorts Board, or the RMC, on an ad hoc basis from time to time.

Particulars

The RMC was a Crown Resorts Board sub-committee with responsibilities relating to risk management and compliance.

158. Crown Resorts, through the RMC and the Crown Resorts Board, made decisions about the risk to be accepted by Crown Melbourne and Crown Perth in relation to designated services provided to international VIP and junket customers on and from 1 March 2016.

159. Those decisions were made in circumstances where:

a. The Crown Resorts Risk Management Policy (**RMP**) did not establish a clear role for the Crown Resorts Board or the RMC with respect to the management of the ML/TF risks of Crown Melbourne or Crown Perth;

Particulars

From October 2016, the RMP set out a high level description of the risk management processes at Crown Resorts and across its wholly-owned operating businesses which included Crown Melbourne and Crown Perth.

b. The Standard Part A Programs did not provide for reporting lines from Crown Melbourne and Crown Perth to the Crown Resorts Board or to the RMC in relation to AML/CTF;

c. The Standard Part A Programs did not specify roles for the Crown Resorts Board or the RMC in relation to ML/TF risk management; and

d. The Crown Melbourne and Crown Perth Boards had not made any determination as to ML/TF risk appetite with respect to international VIP and junket customers.

160. The Standard Part A Programs did not provide an appropriate framework for roles, accountabilities and reporting lines with respect to the management of the ML/TF risks of international VIP and junket customers, for the reasons pleaded at paragraphs 496 to 520 below.

Risk appetite

161. At no time did the Standard Part A Programs include or incorporate appropriate systems and controls for the Crown Melbourne and Crown Perth Boards to:

a. determine their ML/TF risk appetite; and

b. ensure that their business was managed consistent with ML/TF risk appetite.

Particulars

Prior to November 2020, the Crown Resorts Risk Management Strategy (**RMS**) did not include any process for ML/TF risk appetite to be appropriately determined with respect to Crown Melbourne or Crown Perth by Crown Resorts.

On and from June 2019, Crown Resorts had an RMS. The RMS stated that it was the role of the Crown Resorts Board to set the risk appetite for all entities within the group and to oversee its risk management framework.

The RMS stated that the RMC was responsible for overseeing and advising the Crown Resorts Board on Crown Resorts' overall risk appetite, risk culture and risk management strategy. This included responsibility for a consolidated risk profile for all entities, including Crown Melbourne and Crown Perth.

Prior to November 2020, the RMS did not include any process designed to ensure that the Crown Melbourne and Crown Perth businesses were managed consistently with any ML/TF risk appetite.

At no time did the Standard Part A Programs include or incorporate any other process for ML/TF risk appetite to be appropriately determined with respect to Crown Melbourne or Crown Perth.

162. At no time from 1 March 2016 to 1 November 2020 did the Crown Melbourne or Crown Perth Boards determine ML/TF risk appetite for the purposes of the Standard Part A Programs.

Monitoring management performance

163. At no time did the Standard Part A Programs include or incorporate appropriate systems and controls for the Crown Melbourne Board or the Crown Perth Board to appropriately monitor management's performance against an appropriate ML/TF risk management framework, including as against risk appetite.

164. The Crown Melbourne and Crown Perth Boards were unable to have oversight of senior management's performance in mitigating and managing ML/TF risk because:

a. Crown Melbourne and Crown Perth had not set a risk appetite;

b. The Standard Part A Programs did not include or incorporate qualitative and quantitative metrics triggering reporting for material risk categories;

c. The Standard Part A Programs did not include or incorporate processes for monitoring and reporting of Crown Melbourne's and Crown Perth's risk profile relative to quantitative parameters (risk tolerances) against material risk categories;

d. At no time did the Crown Melbourne Board or Crown Perth Board have a documented process in place to ensure in-depth discussion of ML/TF risk as against measurable criteria at regular intervals as part of a rolling agenda; and

e. Prior to November 2020, directors of the Crown Melbourne and Crown Perth Boards were not required to undertake any AML/CTF specific training on appointment, or to complete any refresher training.

165. The Crown Melbourne and Crown Perth Boards and senior management were unable to determine whether risk-based systems and controls required any revision for the purposes of the Standard Part A Programs because:

a. at no time did the Standard Part A Programs include appropriate systems and controls for the Crown Melbourne or Crown Perth Boards to receive and review management reports about new and emerging sources of ML/TF risk or the measures management were taking to deal with those risks;

b. the Standard Part A Programs did not include appropriate systems and controls to detect changes in ML/TF risks, including in both the external and internal environment;

Particulars

See paragraph 129.

c. the Standard Part A Programs did not establish an appropriately resourced and independent AML/financial crime function. This meant that material changes in ML/TF risk could not be consistently identified and escalated to senior management; and

Particulars

See paragraph 177.

d. the Part A Programs did not include appropriate systems and controls to ensure that material changes in ML/TF risk, once identified, were escalated by senior management to the Boards.

Particulars

In the absence of a clearly set ML/TF risk appetite, it was not possible to consistently detect material changes in ML/TF risk.

Senior management accountabilities

166. The Standard Part A Programs did not establish appropriate accountabilities for senior management of Crown Melbourne and Crown Perth with respect to ML/TF risk management and compliance for the reasons pleaded at paragraphs 167 to 173.

Particulars

A Part A program must define risk ownership and assign risk management accountability to senior management to support the consideration of risk in all decision making.

Risk ownership and accountability must be supported by policies, processes, systems and controls to enable senior management to appropriately identify, assess, manage and monitor ML/TF risks reasonably faced by the reporting entity in a manner consistent with the risk appetite set by the Board.

167. At no time did the Standard Part A Programs appropriately define risk ownership and assign risk management accountability with respect to Crown Melbourne and Crown Perth senior management.

Particulars

See clause 3 of the Standard Part A Programs.

168. Prior to November 2020, Crown Melbourne and Crown Perth had a number of management committees with responsibility for risk.

Particulars

These committees included the Crown Melbourne Risk Management Committee (replaced in July 2018 by the Crown Melbourne Executive Risk and Compliance Committee) and the Crown Perth Executive Risk and Compliance Committee.

169. The Standard Part A Programs did not clearly establish the role and accountabilities of these committees with respect to the oversight of ML/TF risk management and compliance.

170. Prior to 1 November 2020, Crown Melbourne and Crown Perth had other management committees with purported responsibility for AML/CTF.

Particulars

The Crown Melbourne committees included the AML/CTF Review Meeting from December 2008 and December 2017. This Meeting was replaced by the AML/CTF Executive Committee, which was in operation until July 2019.

For both Crown Melbourne and Crown Perth, the AML/CTF Committee was established in September 2019, which had its last formal meeting in January 2021.

171. The Standard Part A Programs did not clearly establish the role and accountabilities of these committees with respect to the oversight of ML/TF risk management and compliance.

172. The Standard Part A Programs did not establish appropriate lines of reporting to or from senior management of Crown Melbourne and Crown Perth with respect to ML/TF risk management and compliance.

Particulars

At no time prior to November 2020 did the Part A Programs include or incorporate systems or processes to enable 'top-down' or 'bottom-up' reporting to ensure alignment of ML/TF risk, to identify gaps and to seek appropriate management action to rectify any identified gaps.

173. Prior to November 2020:

a. Crown Melbourne senior management were not required to undertake any AML/CTF specific training.

b. Some Crown Perth senior management undertook AML/CTF specific training, but it was not appropriate for their roles.

Particulars

See paragraph 608 in relation to the adequacy of AML/CTF training provided for through the Standard Part A Programs.

Rule 8.2 of the Rules.

Operational procedures and training for front line business functions

174. At no time did the Standard Part A Programs establish a framework for operational procedures to ensure each Standard Part A Program was capable of being consistently applied by business divisions.

Particulars

For example, there were no appropriately risk-based operational procedures to consistently identify customers who were not low risk; to consistently detect transactions consistent with ML/TF typologies; to detect significant changes in ML/TF risk across the businesses; or to escalate high risk customers to senior management.

175. In the absence of a framework for the consistent application of the Standard Part A Programs, the Crown Melbourne and Crown Perth Boards and senior management were unable to provide appropriate ongoing oversight of the Standard Part A programs.

Particulars

Management cannot appropriately identify, assess, manage and monitor ML/TF risks reasonably faced by the reporting entity in a manner consistent with risk appetite if the Part A program does not include or incorporate policies, processes, systems and internal controls to support and guide business decision making.

By no later than June 2018, the Chief Legal Officer of Crown Resorts, who was also the AMLCO for both Crown Melbourne and Crown Perth, was advised by the Group General Manager AML that the absence of standard operating procedures for the CTRM in Melbourne made any audit of the AML team's work difficult.

176. At no time did the Standard Part A Programs establish appropriate AML/CTF risk awareness training for front line business functions.

Particulars

Rule 8.2 of the Rules.

See paragraph 608.

Some uplift to AML/CTF training did occur from March 2019. However, as Crown Melbourne and Crown Perth did not appropriately identify and assess the ML/TF risk of their business, the AML/CTF Risk Awareness Training remained fundamentally inadequate.

Roles, accountabilities and reporting for the ML/TF risk management and compliance function

177. At no time did the Standard Part A Programs establish an appropriate framework for roles, accountabilities and reporting lines for ML/TF risk management and compliance, for the reasons pleaded at paragraphs 178 to 182.

178. The Standard Part A Programs did not set out an appropriate framework for end-to-end accountabilities for ML/TF risk management or compliance.

Particulars

The Standard Part Programs A did not establish a framework for senior business ownership with respect to AML/CTF processes across all products, customer groups and channels - including ownership with respect to related IT, assurance, reporting and remediation.

179. The Standard Part A Programs did not set out a framework for an appropriately resourced and expert central ML/TF risk management function to monitor, support and challenge the business on ML/TF risk-related matters.

Particulars

The AML and Financial Crime teams were under-resourced and did not receive adequate AML/CTF training. The AML and Financial Crime teams were not supported by appropriate access to senior management and did not have the appropriate authority or opportunity to challenge activities and decisions that could affect the ML/TF risk profile of Crown Melbourne or Crown Perth.

180. The Standard Part A Programs did not establish appropriate and independent reporting lines for AML/CTF from the business and compliance functions up to senior management.

Particulars

It was not until the Financial Crime Compliance & Change Program was approved by the Crown Resorts Board in May 2021 that there was a separation of the Risk and Internal Audit teams, along with elevation of reporting lines and increased resourcing.

See paragraph 711.

181. The Standard Part A Programs did not set out a framework for appropriate assurance and audit functions for AML/CTF matters.

182. At no time did the Standard Part A Programs establish appropriate AML/CTF risk awareness training to support the AML/CTF functions, including at the CTRM/AMLCO levels.

Particulars

Rule 8.2 of the Rules.

See paragraph 608.

Some uplift to training did occur from March 2019. However, as Crown Melbourne and Crown Perth did not appropriately identify and assess the ML/TF risk of their business, the AML/CTF risk awareness Training remained fundamentally inadequate.

Escalation and emerging risks

183. At no time did the Standard Part A Programs include appropriate processes to escalate, mitigate and manage material ML/TF risks.

Particulars

The risk management function should be primarily responsible for monitoring compliance with the Board's articulated risk appetites and risk tolerances and escalating material risk issues to the Board.

Senior management should be primarily responsible for ensuring that appropriate reporting and monitoring processes are developed and implemented to escalate material risk issues from business units to senior management, the risk management function and, if necessary, the Board, including material risk issues identified by external stakeholders.

The Standard Part A Programs did not incorporate or establish appropriate processes.

In the absence of these processes, repeated warnings and 'red flags' raised with senior management of Crown Melbourne, Crown Perth and Crown Resorts were not appropriately escalated. For example, on and from 2014, ANZ, ASB and CBA raised repeated concerns about suspicious patterns of transactions on the **Southbank and Riverbank accounts** that were indicative of money laundering typologies. The Southbank and Riverbank accounts are defined at paragraph 239 below.

No one in the Crown group management reviewed, or directed to be reviewed, the Southbank or Riverbank account statements until August 2019.

184. The Standard Part A Programs did not have any process or procedure to appropriately consider, act on or escalate applicable recommendations or guidance disseminated or published by AUSTRAC.

Particulars

Rule 8.7.

185. At no time did the Standard Part A Programs include appropriate systems and controls to ensure that emerging risks identified through Part A program processes such as transaction monitoring, SMR reporting and ECDD were appropriately escalated to management for the purposes of the ongoing assessment and management of ML/TF risks reasonably faced.

Remediation

186. At no time did the Standard Part A Programs include appropriate systems and controls to identify, review and remediate recurring failures in ML/TF risk management and compliance, as they occurred.

Information management and records

187. At no time did the Standard Part A Programs establish or incorporate an appropriate information management framework to support ML/TF risk management and compliance.

a. Crown Melbourne and Crown Perth did not establish an appropriate framework to create and maintain transaction and customer records.

b. Crown Melbourne and Crown Perth did not establish an appropriate framework to create and maintain transaction and customer records relating to designated services provided through junket channels.

c. Crown Melbourne and Crown Perth did not establish appropriate information or data management systems and controls that were capable by design of supporting:

i. customer risk assessments;

ii. transaction monitoring;

iii. ECDD; and

iv. reporting under Part 3 of the Act.

d. Crown Melbourne and Crown Perth did not establish appropriate procedures to document ML/TF risk management decisions, including relating to ML/TF risk assessments and controls.

188. In the absence of accurate information management, the Crown Melbourne and Crown Perth Boards and senior management could not be assured that they had a full view of significant matters relating to the Standard Part A programs, over which to exercise ongoing oversight.

Crown Perth

189. At all times, ongoing oversight of the Crown Perth casino business was purported to have been conducted through meetings of the Board of Burswood Limited, including with respect to ML/TF risk management and compliance.

Particulars

The Crown Perth Board was the Board of Burswood Nominees Limited.

190. The Crown Perth Standard Part A Program did not establish appropriate reporting on AML/CTF matters from management to the Crown Perth Board or to the Board of Burswood Limited.

a. The Crown Perth Board did not receive regular reports on compliance with the Crown Perth Standard Part A Program.

b. Briefings on the AML reports received by Crown Perth's management level risk committee (**Perth ERCC**) and on the decisions of the Perth ERCC meetings were not provided to the Crown Perth Board or the Board of Burswood Limited.

c. Significant issues from the Perth ERCC were not presented to the Crown Perth Board.

d. The Burswood Limited Board purported to maintain oversight of the Crown Perth Standard Part A Programs through AML/CTF updates generally included in 'internal audit activity' and 'legal, risk and compliance' board reports, which related to matters considered by the Perth ERCC.

e. Significant issues from the Perth ERCC were presented to the Burswood Limited Board, but there was no documented guidance about what should be considered a significant AML/CTF issue and when it should be reported to this Board.

191. The Crown Perth Standard Part A Programs were not subject to appropriate oversight by the Crown Perth Board from 1 March 2016 to 1 November 2020.

Particulars

See paragraph 152.

To the extent that it was appropriate for the Burswood Limited Board to have an oversight role with respect to the Crown Perth Standard

Part A Programs, the programs did not establish an appropriate framework for this oversight role.

192. By reason of the matters pleaded at paragraphs 189 to 191 the Crown Perth Standard Part A Program did not include or establish an appropriate oversight framework for the Part A Program.

Regular independent review

193. Crown Melbourne did not carry out any independent review of its Standard Part A Program in the period 1 March 2016 to 1 November 2020 for the purposes of rule 8.6 of the Rules, as amended from time to time.

194. On 25 January 2016, Crown Melbourne completed an internal audit report that purported to be an independent review for the purposes of rule 8.6 of the Rules.

195. The 25 January 2016 report was not a review that met the requirements of rule 8.6 of the Rules at that time:

a. The review did not assess the effectiveness of the Crown Melbourne Standard Part A Program, having regard to the ML/TF risks of Crown Melbourne, as required by rule 8.6.2(1).

b. The review did not assess whether the Crown Melbourne Standard Part A Program complied with the Rules, as required by rule 8.6.2(2).

c. The review did not assess whether the Crown Melbourne Standard Part A Program had been effectively implemented, as required by rule 8.6.2(3).

d. The review did not assess whether Crown Melbourne had complied with its Standard Part A Program, as required by rule 8.6.2(4).

Particulars

No independent assessment was made of the ML/TF risks reasonably faced by Crown Melbourne or whether the Part A Program, by design, was capable of identifying, mitigating and managing those risks.

Nor was any independent assessment made of whether the Crown Melbourne Standard Part A Program procedures were capable, by design, of meeting the risk-based requirements of the Rules.

The review did not consider the types of designated services provided (including the inherent ML/TF risk), the types of customers that used those services (including the inherent ML/TF risk profile of the customer base), and the channels through which those services were accessed (including the inherent ML/TF risk of the channels).

196. During the period 1 March 2016 to 1 November 2020, Crown Perth completed an internal audit dated 16 February 2018 that purported to be an independent review for the purposes of rule 8.6 of the Rules.

197. The 16 February 2018 report was not a review that met the requirement of rule 8.6.2 of the Rules at that time:

a. The review did not assess the effectiveness of the Crown Perth Standard Part A Program, having regard to the ML/TF risks of Crown Perth, as required by rule 8.6.2(1).

b. The review did not assess whether the Crown Perth Standard Part A Program complied with the Rules, as required by rule 8.6.2(2).

c. The review did not assess whether the Crown Perth Standard Part A Program had been effectively implemented, as required by rule 8.6.2(3).

d. The review did not assess whether Crown Perth had complied with its Standard Part A Program, as required by rule 8.6.2(4).

Particulars

No independent assessment was made of the ML/TF risks reasonably faced by Crown Perth or whether the Standard Part A Program, by design, was capable of identifying, mitigating and managing these risks.

Nor was any independent assessment made of whether the Crown Perth Standard Part A procedures were capable, by design, of meeting the risk-based requirements of the Rules.

The review did not consider the types of designated services provided (including the inherent ML/TF risk), the types of customers that used those services (including the inherent ML/TF risk profile of the customer base), and the channels through which those services were accessed (including the inherent ML/TF risk of the channels).

198. On 23 October 2015, Crown Perth completed an internal audit report that purported to be an independent review for the purposes of rule 8.6 of the Rules at that time. This was not a review that met the requirement of rule 8.6.2 of the Rules for the same reasons pleaded in paragraph 197 above.

The oversight failures - the failure to adopt and maintain a Part A program

199. The absence of a framework for appropriate oversight of ML/TF risk management in the Standard Part A Programs, as pleaded at paragraphs 156 to 198, meant that the Crown Melbourne and Crown Perth Board and senior management, respectively, had no basis to be satisfied that the Standard Part A Programs were operating as intended and that they had the primary purpose of identifying, mitigating and managing the ML/TF risks reasonably faced by the provision of designated services.

Particulars

Section 84(2)(a) of the Act.

200. The absence of a framework for appropriate oversight of ML/TF risk management in the Standard Part A Programs meant that the Crown Melbourne and Crown Perth Board and senior management were unable to exercise ongoing oversight of the Standard Part A Programs.

Particulars

Section 84(2)(c) and of the Act rule 8.4 of the Rules.

201. In the absence of regular independent reviews, the Crown Melbourne and Crown Perth Boards and senior management had no basis to be satisfied that:

a. the Standard Part A Programs were effective having regard to ML/TF risks;

b. the Standard Part A Programs complied with the Rules; or

c. the Standard Part A Programs had been effectively implemented.

Particulars

Section 84(2)(c) of the Act and rule 8.6.5 of the Rules.

Also see rule 8.6.6 from 12 January 2018.

Appropriate risk-based systems and controls

Controls to manage residual risks within appetite

202. Once a reporting entity identifies and assesses its inherent ML/TF risks and determines its risk appetite, the reporting entity must ensure that its Part A program includes appropriate risk-based systems and controls to mitigate and manage residual risks within appetite.

203. These systems and controls must be aligned to and proportionate to the ML/TF risks reasonably faced by the reporting entity with respect to the provision of designated services.

Particulars

Rules 8.1.3 and 8.1.4 of the Rules.

204. Crown Melbourne and Crown Perth did not determine their ML/TF risk appetite and did not determine appropriate Part A program controls to enable designated services to be provided within ML/TF risk appetite.

205. From 1 March 2016 to 1 November 2020, the Standard Part A Programs did not include appropriate risk-based systems and controls that were capable by design of mitigating and managing the ML/TF risks reasonably faced by Crown Melbourne and Crown Perth with respect to designated services they provided for the reasons pleaded at paragraphs 206 to 583 below.

Particulars

Sections 84(2)(a) of the Act and rules 8.1.3 and 8.1.5(4) of the Rules.

See paragraphs 100 to 136 above.

Preventative controls

206. From 1 March 2016 to 1 November 2020, the Standard Part A Programs had very few preventative controls designed to enable Crown Melbourne and Crown Perth to mitigate and manage their ML/TF risks.

Particulars

Preventative controls are those that limit the ability to use a product or channel in a way that would increase the ML/TF risks.

Examples of preventative controls include: setting transactions limits; having a management approval process for high-risk customers, products or countries; applying different identification processes for customers not dealt with in person; or not accepting customers who are deemed too high risk.

207. At all times, the controls in the Standard Part A Programs were predominantly detective and focussed on surveillance for unusual activity that may require SMR reporting to AUSTRAC.

Particulars

Detective controls only seek to monitor activity through a product or channel. Examples of detective controls include: gathering information about how products or channels are used; and reviewing information from internal records, such as transaction monitoring and suspicious matter reporting.

Detective controls do not, of themselves, reduce inherent risks.

The detective controls in the transaction monitoring programs were not appropriately risk-based and did not comply with the Act and Rules. See paragraphs 584 to 651.

Gaming accounts - items 11 and 13, table 3, s6

208. The Standard Part A Programs did not include appropriate risk-based systems and controls that were capable by design of identifying, mitigating and managing the ML/TF risks reasonably faced by Crown Melbourne and Crown Perth with respect to item 11 and 13, table 3, s6 designated services for the reasons pleaded at paragraphs 209 to 279.

DAB accounts and safekeeping accounts

209. At all times, Crown Melbourne and Crown Perth provided customers with DAB accounts and safekeeping accounts.

210. DAB accounts were used by customers for day-to-day transactions involving designated services under table 3, s6 of the Act.

211. At all times, a customer or their representative could deposit value into their DAB account or withdraw value from their DAB account by way of:

a. money in the form of:

   i. cash;

   ii. a transfer to or from a bank account;

   iii. a transfer to or from another DAB account (held by either the customer or a third party);

b. chips or other CVIs; and

c. cheques.

212. Safekeeping accounts were linked to DAB accounts and facilitated the same types of transactions as pleaded at paragraph 211.

213. Safekeeping accounts were also used by customers to:

a. hold partial debt repayments owed to Crown Melbourne or Crown Perth; or

b. 'park' funds (as to which see the matters pleaded at paragraph 251).

214. DAB accounts and safekeeping accounts were maintained by both Crown Melbourne and Crown Perth on SYCO.

215. The opening of DAB accounts and safekeeping accounts constituted item 11 table 3, s6 designated services.

216. Transactions on DAB accounts and safekeeping accounts constituted item 13 table 3, s6 designated services.

217. DAB accounts and safekeeping accounts were a channel through which other table 3, s6 designated services were provided by Crown Melbourne and Crown Perth.

a. A customer could exchange money in a DAB account or safekeeping account for chips or other CVIs (item 7, table 3); or

b. A customer could deposit chips or other CVIs (item 8, table 3) into a DAB account or safekeeping account.

218. DAB accounts and safekeeping accounts were a channel through which table 1, s6 designated services were provided by Crown Melbourne and Crown Perth.

a. Crown Melbourne and Crown Perth provided customers with items 31 and 32, table 1, s6 designated services (remittance services) through DAB accounts.

Particulars

See paragraphs 396 to 423.

b. Credit (by way of a loan) provided to a customer by Crown Melbourne and Crown Perth could be deposited into a customer's DAB account, being items 6, table 1, s6 designated services.

Particulars

See paragraphs 281 to 395.

c. Loan repayments could also be credited to a customer's DAB account, being items 7 and 32, table 1, s6 designated services.

Particulars

See paragraphs 281 to 395.

219. At all times, DAB accounts and safekeeping accounts involved higher ML/TF risks, including:

a. DAB accounts facilitated the movement of money into and out of the casino environment, including through complex transaction chains involving the provision of both table 1 and table 3, s6 designated services.

b. Third parties could deposit funds into DAB accounts and safekeeping accounts by domestic or international telegraphic transfer.

c. Third party cash deposits (via Crown Patron accounts as defined at paragraph 225) could be credited to a customer's DAB account or safekeeping account. These transactions involved the channel risks pleaded at paragraph 238 below.

d. Funds in DAB accounts and safekeeping accounts could be transferred to third parties, by domestic or international telegraphic transfer or by a Crown cheque.

e. Funds could also be transferred from one customer's DAB account or safekeeping account to another customer's DAB account or safekeeping account.

f. A customer could withdraw cash from their DAB account or safekeeping account, including when the customer had applied the funds to minimal or no gaming.

g. Customers (or third parties) could deposit or withdraw funds from DAB accounts or safekeeping accounts through non-face-to-face channels, without being present at the Cage.

Particulars

For example, after returning to their home country, an international customer (or third party) could settle credit owed to Crown Melbourne or Crown Perth by international funds transfer, which was credited to their DAB account.

Where a customer was not on site at the casino, they could request the withdrawal of funds from their DAB account or safekeeping account through an Authority to Disperse Form, including by way of transfer to a third party.

On 8 April 2020, Crown Melbourne and Crown Perth circulated a memorandum stating that it would no longer make or receive payments to or from third parties without prior written approval from the relevant Chief Operating Officer and Group General Manager AML. This policy was not formalised until October 2020. It was not until 16 November 2020 that manual weekly reviews commenced to identify deposits from third parties.

h. As pleaded at paragraph 680 below, Crown Melbourne and Crown Perth provided customers with multiple DAB accounts, sometimes with different customer (or patron) identification numbers (known as **PIDs**). Funds could be transferred between these accounts.

i. DAB accounts and safekeeping accounts could be used to 'park' funds, as pleaded at paragraph 251 below.

220. Crown Melbourne and Crown Perth did not conduct an appropriate assessment of the ML/TF risks of providing table 1, s6 designated services through DAB accounts and safekeeping accounts.

221. Crown Melbourne and Crown Perth did not conduct an appropriate assessment of the ML/TF risks of providing table 3, s6 designated services through DAB accounts and safekeeping accounts.

222. The Standard Part A Programs did not include appropriate risk-based systems and controls that were capable by design of identifying, mitigating and managing the ML/TF risks reasonably faced by Crown Melbourne and Crown Perth with respect to designated services provided through DAB accounts and safekeeping accounts.

a. The Standard Part A Programs did not include appropriate risk-based systems and controls to identify, mitigate and manage the ML/TF risks identified at paragraph 219 above.

b. Crown Melbourne and Crown Perth did not impose a limit on the amount of money that a customer could hold in a DAB account or safekeeping account.

c. There was no limit on telegraphic transfers into or out of a DAB account or safekeeping account, or on cash withdrawals.

d. Prior to November-December 2018, Crown Melbourne and Crown Perth did not impose a limit on the amount of money that a customer could transfer into or out of a DAB account or safekeeping account in a single transaction (subject to paragraph e below).

e. From November-December 2018 until 11 November 2020, a $300,000 cap on cash transactions in any 24 hour period was introduced for junket operators, junket representatives and key players. This control did not apply to non-cash transactions.

f. It was not until November 2020 that limits were placed on other cash deposits. From November 2020, cash deposits over $250,000 (in aggregate across a calendar day or in a single transaction) were no longer permitted at the Cage. On 18 February 2021, the $250,000 limit was reduced to $200,000, and to $150,001 on 21 May 2021.

223. The failure to appropriately identify, mitigate and manage the ML/TF risks of DAB accounts and safekeeping accounts made Crown Melbourne and Crown Perth vulnerable to criminal exploitation.

224. At 15 June 2021 Crown Melbourne held $47.1 million of customers' monies, comprising:

a. $22 million in 2,438 DAB accounts; and

b. $25.1 million in 89 safekeeping accounts.

The Crown Patron account channel

225. Crown Melbourne and Crown Perth maintained bank accounts (**Crown Patron accounts**) to facilitate the transfer of funds into DAB accounts and safekeeping accounts:

a. At all times, Crown Melbourne maintained up to:

i. 8 accounts in Australian dollars; and

ii. 15 foreign currency accounts.

b. At all times, Crown Perth maintained up to:

i. 4 accounts in Australian dollars; and

ii. 7 foreign currency accounts.

226. Crown Patron accounts were used by both domestic and international customers of Crown Melbourne and Crown Perth to move money into the casinos.

227. Crown Patron accounts were used by some corporate entities to make deposits on behalf of Crown Melbourne and Crown Perth customers, including:

a. corporate entities run by junket tour operators;

b. overseas deposit services to deposit funds on behalf of customers; and

c. third parties such as remittance service providers to deposit funds on behalf of customers.

Particulars

See paragraphs 332 to 395.

See the particulars at paragraph 219.

228. Transfers into DAB accounts and safekeeping accounts via the Crown Patron accounts involved the provision of item 32, table 1, s6 designated services by Crown Melbourne and Crown Perth, including both domestic and international remittance.

229. Transactions on DAB accounts and safekeeping accounts are item 13, table 3 s6 designated services.

230. The Crown Patron accounts were a channel through which Crown Melbourne and Crown Perth provided:

a. item 13, table 3, s6 designated services on DAB accounts and safekeeping accounts; and

b. item 32, table 1, s6 designated services.

231. Customers could deposit funds into Crown Patron accounts by:

a. non-face-to-face direct transfer, both from:

i. within Australia; or

ii. another country; or

b. deposit at the Cage.

232. Funds could be deposited into a Crown Patron account by cash, cheque or telegraphic transfer, in Australian dollars or foreign currency.

233. A customer of Crown Melbourne or Crown Perth could:

a. deposit funds personally into a Crown Patron account;

b. arrange for any third party to deposit funds into a Crown Patron account;

c. instruct another casino (Australian or foreign) to transfer funds from their non-Crown casino account into a Crown Patron account; and

d. instruct another Crown entity to deposit funds into a Crown Patron account on their behalf.

Particulars

For example, a Crown Perth or Crown Aspinalls, London, customer could arrange for funds to be deposited into a Crown Patron account to be made available for gaming at Crown Melbourne and vice-versa.

See the particulars at paragraph 219.

234. Prior to September 2020, deposits by or on behalf of customers into Crown Patron accounts were attributed to a customer of Crown Melbourne or Crown Perth in two ways:

a. The **Credit Control team** (within VIP International, Crown Resorts) accessed the online bank statements for the Crown Patron accounts, checked for new deposits for

the previous day, and provided the Cage team with a record of the transaction (**Transaction Record**). The Cage team used the Transaction Record to credit deposits from the Crown entity account into the customer's DAB account or safe keeping account.

b. Alternatively, a customer could present a copy of the transfer receipt to the Cage evidencing the transfer from the customer's personal bank account. The Cage staff verified the receipt against the transaction records from the online bank account and credited the deposit against the customer's DAB account or safekeeping account.

c. The credit of funds to the DAB account or safekeeping account was an item 32, table 1, s6 designated service.

235. After September 2020, deposits by or on behalf of customers into Crown Patron accounts were attributed to a customer of Crown Melbourne or Crown Perth as follows:

a. When a customer sought to access any funds they had transferred to a Crown patron account, the Cage team requested a receipt from the customer evidencing the transfer, checked that it complied with Crown's policies and matched the receipt with the bank statements for the Crown Patron account.

b. If these checks were confirmed, the Cage team authorised the transfer to the customer's DAB account or safekeeping account through a Telegraphic Transfer Acknowledgement (**Transfer Acknowledgement**).

c. The credit of funds to the DAB account or safekeeping account was an item 32, table 1, s6 designated service and an item 13, table 3, s6 designated service.

236. Once the process at either paragraph 234 or 235 had been completed, a customer of Crown Melbourne or Crown Perth could access funds deposited into a Crown Patron account at the Crown Melbourne or Crown Perth Cage via their DAB account or safekeeping account as follows:

a. obtaining chips or other CVI (items 7 and 13, table 3, s6 designated services) at the Cage;

b. withdrawing cash in Australian dollars or foreign currency (item 13, table 3, s6 designated services) at the Cage; and/or

c. loading the value onto the customer’s Crown Rewards card (item 13, table 3, s6 designated services), which could then be transferred to a Card Play Extra account, as to which see the matters pleaded at paragraphs 255 to 279 below.

237. Once funds had been deposited into a DAB account or a safekeeping account, including via the Crown Patron account channel, a customer could instruct Crown Melbourne and Crown Perth to:

a. transfer the funds to another bank account, including the customer’s personal account, a third party bank account or a bank account of another casino;

b. transfer the funds to another Crown affiliated entity (including Crown Melbourne, Crown Perth or Crown Aspinalls);

c. transfer the funds to another customer’s DAB account or safekeeping account;

d. Each of the transfers pleaded at a. to c. from a DAB or safekeeping account was an item 31, table 1, s6 designated service and an item 13, table 3, s6 designated service.

Particulars

See the particulars at paragraph 219.

238. The provision of item 13, table 3 and item 32, table 1 s6 designated services through the Crown Patron account channel involved higher ML/TF risks, including risks arising by reason of the following:

a. Designated services provided through the Crown Patron account channel were facilitated through DAB account and safekeeping accounts, which involved the ML/TF risks pleaded at paragraph 219.

b. Funds could be deposited into Crown Patron accounts through non-face-to-face channels.

c. Funds could be deposited into Crown Patron accounts offshore, including in foreign currencies.

d. Funds could be moved across international borders through Crown Patron accounts.

e. Crown Melbourne and Crown Perth had very limited visibility over who was depositing funds into Crown Patron accounts.

f. Crown Melbourne and Crown Perth conducted no, or very limited, checks to identify the party depositing funds and their source of funds.

g. Crown Melbourne and Crown Perth accepted cash deposits through Crown Patron accounts.

h. Crown Patron accounts held with CBA permitted 'QuickCash' deposits, whereby the person depositing the cash could place the cash with a deposit slip into a sealed envelope and deposit the funds via a QuickCash chute or QuickCash Safe.

i. Crown Melbourne and Crown Perth accepted deposits into Crown Patron accounts from third parties (both telegraphic transfer and cash).

j. Acceptance of third party payments into Crown Patron accounts provided an avenue for money laundering through smurfing or cuckoo smurfing.

k. Once funds were deposited into a DAB accounts or safekeeping account via the Crown Patron account channel, the funds could be transferred out of the DAB or safekeeping account through further transactions, including as follows.

l. A customer could access deposited funds at the Cage by way of cash withdrawal from their DAB account, whether or not they used these funds to gamble.

m. A customer could access funds through non-face-to-face channels including by requesting a transfer of funds from their DAB account or safekeeping account, to another bank account in their own name or in the name of a third party, whether or not they used these funds to gamble.

n. A customer could move funds deposited in Crown Patron accounts from a Crown Rewards Card to a Card Play Extra account.

239. The Southbank and Riverbank Crown Patron account channels posed particularly high ML/TF risks:

a. The **Southbank accounts** were accounts in the name of Southbank Investments Pty Ltd operated by Crown Melbourne, that were used, or that were capable of being used,

for the purpose of depositing, transferring or withdrawing funds for Crown Melbourne customers.

b. The **Riverbank accounts** were accounts in the name of Riverbank Investments Pty Ltd operated by Crown Perth, that were used, or that were capable of being used, for the purpose of depositing, transferring or withdrawing funds for Crown Perth customers.

c. The Southbank and Riverbank accounts were established in around 2001 to give VIP customers 'privacy' in moving money.

d. Junket operators used these accounts, as did money remitters, overseas deposit services and individuals.

Particulars

See paragraphs 332 to 395.

e. These accounts were not transparent because:

   i. they were in the name of shell companies, with their connection to Crown Melbourne and Crown Perth not apparent on their face; and

   ii. some customer deposits were entered with the description 'investment', disguising their purpose.

f. On several occasions from January 2014, banks put Crown Melbourne and Crown Perth on notice that money laundering may have been occurring through the Southbank and Riverbank accounts, as follows:

   i. The banks advised that structuring appeared to be occurring on the accounts and that the identities of numerous depositors were unknown.

   ii. The accounts were closed first by HSBC in 2013, and then by ANZ in 2015 and by CBA in 2019.

g. The concerns raised by banks as pleaded at f. were not escalated to Crown Resorts' RMC, the Crown Melbourne Board, or the Crown Perth Board until December 2019.

h. No one in the Crown group management reviewed, or directed to be reviewed, the Southbank or Riverbank account statements until August 2019.

i. An external auditor's report concluded that the value of deposits into the Southbank and Riverbank accounts between 2013 and 2019, with features indicative of money laundering, was over $290 million.

Particulars

Transactions on the Southbank and Riverbank accounts were identified as being indicative of possible structuring and cuckoo smurfing.

Apparent structuring on the Southbank accounts alone totalled $1,873,157 from 2014 to 2021. A significant proportion of these structured transactions were conducted by junket operators.

Most of the potential structuring on the Southbank accounts was also identified as potential smurfing activity.

From February 2014 to December 2019 a total of $63,521,892 was deposited into the Southbank accounts by (individual) third parties on behalf of customers and $45,867,456 was deposited into these accounts by (corporate) third party agents.

j. The Southbank and Riverbank accounts were at risk of being exploited by organised crime.

240. Crown Melbourne and Crown Perth failed to assess the ML/TF risks of providing item 13, table 3, s6 designated services through the Crown Patron accounts channel.

241. Crown Melbourne and Crown Perth failed to assess the ML/TF risks of providing item 32, table 1, s6 designated services through the Crown Patron accounts channel.

242. The Standard Part A Programs did not include appropriate risk-based systems and controls that were capable by design of identifying, mitigating and managing the ML/TF risks reasonably faced by Crown Melbourne and Crown Perth with respect to designated services provided on DAB accounts and safekeeping accounts through the Crown Patron account channels, including for the following reasons:

a. The Standard Part A Programs did not include appropriate risk-based controls to identify, mitigate and manage the ML/TF risks pleaded at paragraphs 238 and 239.

b. The Standard Part A Programs had no risk-based processes in place to understand the source of funds of transactions through the Crown Patron account channel.

c. Crown Melbourne and Crown Perth accepted deposits through Crown Patron accounts from third parties with no or very limited checks as to the identity of the third party or their source of funds.

d. The Standard Part A Programs had no processes to identify deposits into Crown Patron accounts that were made in cash.

e. Detective controls applied to deposit of funds into DAB accounts and safekeeping accounts through the Crown Patron account channel were inadequate.

Particulars

By no later than June 2018, the Chief Legal Officer of Crown Resorts, who was also the AMLCO for both Crown Melbourne and Crown Perth, was advised by the Group General Manager AML that Crown Melbourne will accept third party deposits into DAB accounts with very limited checks as to the identity of the third party or their source of funds. The Chief Legal Officer/AMLCO was advised there was a potential vulnerability that these third party deposits were from an illicit source.

The briefing recommended that Crown Melbourne's willingness to accept third party transfers and/or deposits without conducting further KYC or other due diligence to understand the source of funds be taken to the Crown Melbourne Board for consideration, as it raised questions of risk appetite.

See the particulars at paragraphs 219 and paragraph 593.

243. The failure to appropriately identify, mitigate and manage the ML/TF risks of providing designated services through the Crown Patron account channel made Crown Melbourne and Crown Perth vulnerable to criminal exploitation.

The Hotel Card channel - Crown Melbourne

244. From 1 March 2016 to October 2016, Crown Melbourne adopted a practice of:

a. receiving money at Crown Towers Hotel Melbourne from international VIP customers through the customer's credit or debit card; and

b. making the money available to the customer for gaming at the Crown Melbourne Casino

(the **HCT channel**).

245. The HCT channel commenced in about August 2012.

246. Money processed through the HCT channel could be accessed by the customer at the Crown Melbourne Casino as follows:

a. The money could be deposited into the customer's DAB account, being an item 13, table 3, s6 designated service.

b. The money could be redeemed by a Chip exchange voucher (**CEV**) or Chip purchase voucher (**CPV**).

247. The provision by Crown Melbourne of designated services through the HCT channel involved higher ML/TF risks including because:

a. the HCT channel lacked transparency;

b. of the jurisdictional profile of the customers involved;

c. of the risk it was facilitating capital flight;

d. money deposited in DAB accounts could be withdrawn in cash;

e. money deposited in DAB accounts could be transferred to third parties;

f. a significant proportion of withdrawal activity connected to HCT deposits were remitted to junket operators.

248. At no time did Crown Melbourne carry out an ML/TF risk assessment of DAB deposits through the HCT channel.

249. The Crown Melbourne Standard Part A Program did not include appropriate risk-based systems and controls that were capable by design of identifying, mitigating and managing the ML/TF risks reasonably faced by Crown Melbourne with respect to designated services provided on DAB accounts and safekeeping accounts through the HCT channel, for the following reasons:

a. In the absence of an assessment of the ML/TF risks of the HCT channel, the risk-based preventive and detective controls throughout Crown Melbourne's Standard Part A Programs were not designed to manage and mitigate the ML/TF risks specific to the HCT channel, as required by the Act and Rules.

b. In particular, transaction monitoring and subsequent suspicious matter reporting undertaken by Crown Melbourne was focussed on broader customer transactional activity and predominantly on transactions that were downstream of the HCT channel.

c. As a result of the matters pleaded at a. and b., the controls in Part A did not identify, assess or report ML/TF risks presented by the channel or by the origin of the HCT funds.

250. Just under $161 million was deposited through the HCT channel from August 2012 to October 2016, with over $50 million being deposited after 1 March 2016.

Dormant or parked funds in DAB accounts and safekeeping accounts

251. At all times prior to 1 November 2020, a customer of Crown Melbourne or Crown Perth could leave unlimited funds in a DAB or safekeeping account for an unlimited period without applying those funds to gaming (**parked or dormant funds**).

252. Parked or dormant funds in DAB or safekeeping accounts posed higher ML/TF risks for the following reasons:

a. A DAB or safekeeping account having large dormant balance, of itself, was an indicator of ML/TF risk as it is contrary to the purposes of such accounts.

b. DAB and safekeeping accounts could be used to store money outside the banking system.

c. The 'parking' of illicit money puts distance between the act or acts that generated the illicit funds and the ultimate recipients of those funds, making it harder to understand or trace the flow of money.

d. Gaming accounts such as DAB accounts or safekeeping accounts could be used to park or hide funds from law enforcement and relevant authorities.

e. A customer who held a large dormant balance in a DAB or safekeeping account may have had a higher risk profile that may have required closer or enhanced customer due diligence including analysis as to the source of funds or wealth.

f. DAB accounts or safekeeping accounts held by junket operators or representatives were highly vulnerable to the storage and movement of potentially illicit funds.

Particulars

See paragraph 477 below.

g. A DAB account or safekeeping account that held a large dormant balance, with minimal gaming by the customer, could involve higher ML/TF risks.

h. The use of DAB accounts for predominantly financial transactions, namely the movement of money into and out of the casinos, represented a higher ML/TF risk.

i. Large withdrawals from a previously dormant account could indicate higher ML/TF risks.

253. An external auditor identified 42 large holding balances in either DAB or safekeeping accounts maintained by Crown Melbourne and Crown Perth, being balances greater than $50,000 and dormant for at least 90 days, during the period 2016 to 30 April 2021:

a. These 42 accounts related to 41 different customers

b. Six balances, in accounts maintained by Crown Melbourne, were identified to be greater than $1,000,000. These accounts were in the names of Customer 31, Customer 21, Customer 52, Customer 50, Customer 7 and Customer 18.

c. The average dormancy period for the 42 balances was 593 days, with the longest period of dormancy being 1,921 days for an account in the name of Customer 7.

d. Background checks and adverse media searches conducted by the external auditor for the 41 customers showed potential matches for several customers in relation to money laundering, bribery, links to organised crime, embezzlement, fraud or other criminal activity.

254. The Standard Part A Programs did not include appropriate risk-based systems and controls that were capable by design of identifying, mitigating and managing the ML/TF risks reasonably faced by Crown Melbourne with respect to parked or dormant funds on DAB accounts and safekeeping accounts, for the following reasons:

a. Crown Melbourne and Crown Perth did not apply appropriate risk-based monitoring of dormant or parked funds in DAB accounts and safekeeping accounts to identify, mitigate and manage the ML/TF risks pleaded at paragraph 252 above.

b. At no time did the Standard Part A Programs enable Crown Melbourne or Crown Perth to conduct appropriate due diligence on customers with dormant or parked balances in DAB or safekeeping accounts.

Particulars

By no later than June 2018, the Chief Legal Officer of Crown Resorts, who was also the AMLCO for both Crown Melbourne and Crown Perth, was advised by the Group General Manager AML (Crown Melbourne) that that the AML Team in Melbourne infrequently checked accounts for parked monies.

It was not until October 2021 that Crown implemented a Return of Funds Policy to manage dormant accounts with positive balances, which is yet to be adopted and implemented.

Card Play Extra accounts

255. At all times Crown Melbourne and Crown Perth offered customers accounts that facilitated play on electronic gaming machines (**EGMs**) or electronic table games (**ETGs**):

a. Crown Melbourne called these accounts **Card Play**.

b. Crown Perth called these accounts **Cashless accounts**.

Particulars

See paragraphs 429 to 435 below with respect to designated services provided through EGMs and ETGs.

256. Any Crown Melbourne customer who:

a. joined Crown Rewards; and

b. accumulated loyalty points for play

could be provided with a Card Play account.

257. Any Crown Perth customer:

a. with a minimum Gold tier membership for Crown Rewards; and

b. who was a member of the Pearl Room

could be provided with a Cashless account facility.

258. The Card Play and Cashless accounts facilitated the transfer of credits between a customer's Crown Rewards card and EGMs.

259. The Card Play and Cashless accounts facilitated the provision of item 6 and 9, table 3, s6 designated services.

260. Crown Melbourne and Crown Perth provided item 11, table 3, s6 designated services when they opened a Card Play or a Cashless account for a customer.

261. The deposit of credit on Card Play and Cashless accounts, transferred from a Crown Rewards card or EGM, was an item 13, table 3, s6 designated service.

262. Credits on Card Play and Cashless accounts could be cashed out by:

a. collecting a ticket from an EGM or ETG; and then either

b. cashing the ticket out at the Cage; or

c. at a ticket redemption terminal (**TRT**) (in the case of a Card Play account at Crown Melbourne only).

263. Crown Melbourne and Crown Perth provided item 13, table 3, s6 designated services when credits on a Card Play and Cashless account were cashed out.

264. Card Play Extra accounts at Crown Melbourne were Card Play accounts with added functionality that allowed customers to:

a. deposit money, including cash, into a Card Play Extra account; and

b. withdraw money, including cash, from a Card Play Extra account.

265. All Cashless accounts at Crown Perth had the functionality pleaded at paragraph 264. **Card Play Extra account**, as used in this Statement of Claim, refers to both Card Play Extra accounts at Crown Melbourne and Cashless accounts at Crown Perth.

266. Funds could be deposited to a Card Play Extra account by:

a. presenting the Crown Rewards membership card at the Cage and depositing cash using the customer PIN;

b. withdrawing funds from the customer's DAB account and transferring them over to the Card Play Extra account; or

c. for Crown Melbourne customers only, inserting the membership card into a TRT, entering the Crown Rewards customer PIN and inserting cash up to a maximum of $2,000 per transaction.

267. Funds deposited by a customer of Crown Melbourne or Crown Perth into a Crown Patron account could also be loaded onto the customer's Crown Rewards card, which could then be transferred to a Card Play Extra account: see paragraph 236 above.

268. Cash could be withdrawn from a Card Play Extra account at:

a. a TRT, up to $2,000 per transaction (at Crown Melbourne only); or

b. the Cage.

269. Credits could be withdrawn from a Card Play Extra account in the same way described at paragraph 262 above.

270. Deposits and withdrawals on Card Play Extra accounts were item 13, table 3, s6 designated services.

271. The maximum amount a customer could deposit into, or withdraw from, a Card Play Extra account at the Cage depended on their tier level of membership with Crown Rewards.

272. Each Crown Rewards membership tier had a maximum card balance.

273. The following limits applied in respect of each Crown Rewards membership tier for Crown Melbourne:

a. Member Tier – Maximum Card Balance – $2,000;

b. Silver Tier – Maximum Card Balance – $2,000;

c. Gold Tier – Maximum Card Balance – $50,000;

d. Platinum Tier – Maximum Card Balance – $75,000;

e. Black Tier – Maximum Card Balance – $250,000; and

f. Exclusive Black Tier – Maximum Card Balance – $500,000.

274. The following limits applied in respect of each Crown Rewards membership tier for Crown Perth:

a. Gold Tier – Maximum Card Balance – $40,000; and

b. Platinum Tier and Black Tier – Maximum Card Balance – $100,000.

275. Money deposited into Card Play Extra accounts could be used to facilitate the provision of item 6 table 3, s6 designated services on EGMs and ETGs.

276. Having entered into a game on an EGM or ETG (item 6, table 3, s6), a customer could be paid out winnings (item 9, table 3, s6) in the form of a ticket, including where there was minimal to no play.

277. In November 2016, Crown Melbourne approved an increase to the amount that was to be printed on tickets of up to:

a. $20,000 for restricted EGMs;

b. $20,000 for unrestricted EGMs and ETGs outside a private gaming room known as the Mahogany Room; and

c. $75,000 for unrestricted EGMs and ETGs within the Mahogany Room.

278. Crown Melbourne and Crown Perth did not conduct an appropriate assessment of the ML/TF risks of providing designated services through Card Play Extra accounts.

Particulars

Crown Melbourne and Crown Perth did not adequately assess the ML/TF risks of cash deposits and withdrawals, including with respect to the risks posed by the tier limits.

279. At no time did the Standard Part A Programs include appropriate risk-based systems and controls that were capable by design of identifying, mitigating and managing the ML/TF risks reasonably faced by Crown Melbourne and Crown Perth with respect to Card Play Extra accounts.

a. Deposits and withdrawals using Card Play Extra were recorded against the customer's PID in the EzPay system, which is not linked to SYCO. Transaction monitoring was accordingly not capable of being applied to these transactions.

b. With respect to the Card Play Extra accounts, the Standard Part A Programs did not include appropriate:

i. transaction limits or daily limits on cash deposits or withdrawals;

ii. limits on account balances;

iii. limits or controls on the cashing out of tickets issued from Card Play Extra credits;

iv. controls to identify whether money was being withdrawn from the Card Play Extra account with little or no play;

v. controls with respect to the channels through which funds could be deposited into Card Play Extra accounts, including DAB deposits via channels such as the Crown Patron account channel.

Particulars

By no later than June 2018, the Chief Legal Officer of Crown Resorts, who was also the AMLCO for both Crown Melbourne and Crown Perth, was advised by the Group General Manager AML (Crown Melbourne) that there was little or no oversight of the Card Play Extra account by Crown Melbourne, and that it was not covered by either the Crown Melbourne Standard Part A Program or the Crown Perth Standard Part A Program. The Group General Manager AML recommended that the Standard Part A Program be updated to cover the Card Play Extra account.

Loans - items 6 and 7, table 1, s6

280. The Standard Part A Programs did not include appropriate risk-based systems and controls that were capable by design of identifying, mitigating and managing the ML/TF risks reasonably faced by Crown Melbourne and Crown Perth with respect to item 6 and 7, table 1, s6 designated services for the reasons pleaded at paragraphs 281 to 395 below.

Credit facilities - item 6, table 1, s6 designated services

281. At all times:

a. Crown Melbourne provided credit facilities to customers; and

b. Crown Perth provided credit facilities to customers, up to 23 February 2021.

Particulars

Credit facilities were available to international customers participating in a junket or Premium Player Program.

Crown Perth referred to credit facilities as funds advance facilities.

282. A customer applied for a credit facility by completing and signing a form titled 'International Crown Melbourne and Crown Perth Application for a Deposit Account, Cheque Cashing, or Credit Facility/Funds Advance Facility' (the **International credit facility application**).

283. The international credit facility application included an application for a credit facility limit.

284. If the application and credit facility limit was approved, an employee authorised by both Crown Melbourne and Crown Perth signed the application.

285. The application form, once signed by the applicant, and approved and signed by the authorised employee, operated as an agreement between Crown Melbourne and Crown Perth, and the applicant (the **International Credit Facility Agreement**).

286. Once an International Credit Facility Agreement was approved, the customer could access funds up to the approved limit at either Crown Melbourne or Crown Perth.

287. Crown Melbourne and Crown Perth made a loan to a customer upon the execution of an International Credit Facility Agreement with respect to the credit facility.

Particulars

A credit facility was an advance of money by Crown Melbourne or Crown Perth to the customer.

Paragraph (a) of the definition of 'loan' in s5 of the Act

288. At all times, Crown Melbourne and Crown Perth made loans as described at paragraph 287 in the course of carrying on a loans business.

Particulars

The provision of credit facilities as loans was a 'core activity' of the Crown Melbourne and Crown Perth businesses that facilitated the generation of gaming revenue.

The provision of credit facilities involved systemisation and repetition.

Credit Facilities were primarily provided to junkets and international VIPs. Credit for these international customers facilitated high value gaming. The International VIP business was a significant component of Crown Melbourne and Crown Perth's revenue.

289. At all times, the execution of an International Credit Facility Agreement by Crown Melbourne and Crown Perth with respect to the credit facility involved the provision of an item 6, table 1, s6 designated service to the customer.

Credit facilities - item 7, table 1, s6 designated services

The drawdown of funds under a credit facility

290. A customer could draw on an approved credit facility at the Crown Melbourne or Crown Perth casino premises.

291. A customer could draw down on a credit facility in a number of ways:

a. A customer could be issued with a CPV, gaming chips, cash, or cash equivalent; or

b. Where a credit facility was linked to a DAB account, the amount drawn down could be deposited into the customer's DAB account.

(the **drawdown of funds from a credit facility**).

292. When a customer drew down on funds from their credit facility by any one of the means pleaded at paragraph 291:

a. Crown Melbourne would issue a 'credit marker' in the amount of the funds drawn;

b. Crown Perth would issue a 'draw down marker' in the amount of the funds drawn.

(**collectively referred to as credit markers**).

293. A credit marker was a non-bankable instrument issued by Crown Melbourne or Crown Perth to recognise the amount owed to Crown Melbourne or Crown Perth by the customer.

294. A credit marker was issued for a 20 banking day period from the date of issuance (unless executive management provided approval to either extend or reduce the period).

295. The credit marker was issued in the currency that the customer's junket or Premium Player Program was opened.

296. Crown Melbourne and Crown Perth could also issue a **substitution voucher** to replace a credit marker with a personal or company cheque for the same value.

297. A customer could draw on the credit facility on multiple occasions within the facility limit, rather than once in respect of the full amount of the facility limit. Each drawdown was recorded on a credit marker.

298. A drawdown of funds from a credit facility was a transaction in relation to a loan where the loan was made in the course of carrying on a loans business.

Particulars

See the particulars at 288.

299. Crown Melbourne and Crown Perth provided an item 7, table 1, s6 designated service when they provided a customer with a drawdown of funds from a credit facility.

Particulars

See paragraph 291.

The redemption of a credit marker

300. A customer could redeem a credit marker (or repay funds owed to Crown Melbourne or Crown Perth under a credit facility) in a number of ways, including by:

a. a cash payment at the Cage by the customer;

b. domestic or international telegraphic transfer to Crown Melbourne or Crown Perth by the customer;

c. domestic or international telegraphic transfer to Crown Melbourne or Crown Perth by a third party;

d. applying gaming chips, CPVs, or cash equivalents held by the customer;

e. transferring funds from the customer's DAB account;

f. a set-off of winnings by the customer at either Crown Melbourne or Crown Perth; or

g. other set-offs, as agreed.

Particulars

See the particulars at paragraph 219.

301. The redemption of a credit marker (or the acceptance of a repayment by Crown Melbourne and Crown Perth under a credit facility) was a transaction in relation to a loan where the loan was made in the course of carrying on a loans business.

Particulars

See paragraph 288.

302. Crown Melbourne and Crown Perth provided an item 7, table 1, s6 designated service when they redeemed a credit marker (or accepted a repayment under a credit facility).

Cheque cashing facilities - item 6, table 1, s6 designated services

303. At all times, Crown Melbourne and Crown Perth provided Cheque Cashing Facilities (**CCFs**) to customers.

Particulars

CCFs were available to both domestic and international customers.

304. An international customer applied for a CCF by completing and signing the same form described at paragraph 282 above (the International credit facility application).

305. A domestic customer applied for a CCF at:

a. Crown Melbourne by completing and signing a form titled 'Domestic Application for a CCF (including a Deposit Account)'; and

b. at Crown Perth by completing a form titled 'Crown Perth Domestic Application for Deposit/Cheque Cashing Facility'

(collectively, the **domestic CCF application**).

306. The international credit facility application and domestic CCF applications each included an application for a facility limit.

307. If an international credit facility application and facility limit was approved and an agreement executed, as described at paragraphs 284 to 285 above, the customer could access both the credit facilities and a CCF up to the approved limit at Crown Melbourne and/or Crown Perth.

308. The domestic CCF application form, once signed by the applicant, and approved and signed by the authorised employee, operated as an agreement between Crown Melbourne and Crown Perth, and the applicant (the **domestic CCF Agreement**).

309. Once a domestic CCF Agreement was approved by Crown Melbourne, the customer could access funds up to the approved limit at Crown Melbourne only.

310. Once a domestic CCF Agreement was approved by Crown Perth, the customer could access funds up to the approved limit at Crown Perth only.

311. Crown Melbourne and Crown Perth made a loan to a customer upon the execution of an International Credit Facility Agreement with respect to the CCF.

Particulars

A CCF was an advance of money by Crown Melbourne or Crown Perth to the customer.

Paragraph (a) of the definition of 'loan' in s5 of the Act.

312. Crown Melbourne and Crown Perth made a loan to a customer upon the execution of a domestic CCF Agreement.

Particulars

A CCF was an advance of money by Crown Melbourne or Crown Perth to the customer.

Paragraph (a) of the definition of 'loan' in s5 of the Act.

313. At all times, Crown Melbourne and Crown Perth made loans as described at paragraphs 311 and 312 in the course of carrying on a loans business.

Particulars

The provision of CCFs was a 'core activity' of the Crown Melbourne and Crown Perth businesses that facilitated the generation of gaming revenue.

The provision of CCFs involved systemisation and repetition.

The provision of CCFs facilitated the provision of table 3 s6 gaming services to a material number of high value customers.

314. At all times the execution of:

a. an International Credit Facility Agreement by Crown Melbourne and Crown Perth with respect to the CCF; and

b. a domestic CCF Agreement

involved the provision of an item 6, table 1, s6 designated service to the customer.

Cheque cashing facilities - item 7, table 1, s6 designated services

The drawdown of funds under a CCF

315. A customer could draw on an approved CCF at the Crown Melbourne or Crown Perth casino premises.

316. A customer could draw down on a CCF in a number of ways:

a. A customer could be issued with a CPV, gaming chips, cash, or cash equivalent; or

b. Where a CCF facility was linked to a DAB account, the amount drawn down could be deposited into the customer's DAB account.

(**the drawdown of funds under a CCF**).

317. When a customer drew down on funds from their CCF by any one of the means pleaded at paragraph 316:

a. The customer would present one or more personal cheques to the Crown Melbourne or Crown Perth Cage - provided the total of the amount made out on the cheque was less than or equal to the approved facility limit of the CCF; or

b. The customer would be issued with a 'counter cheque' at the Crown Melbourne or Crown Perth Cage - up to an amount that was less than or equal to the approved facility limit of the CCF.

318. A counter cheque was a document issued by Crown Melbourne or Crown Perth that:

a. included a customer's bank account details;

b. was bankable;

c. was generated at the Cage or a gaming table location; and

d. was drawn against a customer's approved CCF.

319. Crown Melbourne and Crown Perth could also issue a substitution voucher to replace a counter cheque with a personal or company cheque for the same value.

320. A drawdown of funds from a CCF was a transaction in relation to a loan where the loan was made in the course of carrying on a loans business.

Particulars

See the particulars at paragraph 313.

321. Crown Melbourne and Crown Perth provided an item 7, table 1, s6 designated service when they provided a customer with a drawdown of funds from a CCF.

Particulars

See paragraph 316.

Repayments under a CCF

322. A customer could repay funds owed to Crown Melbourne or Crown Perth under a CCF in the ways pleaded at paragraphs 323 to 326 and 329.

323. Where a domestic customer used a personal cheque to draw down funds under a CCF, the cheque was banked no later than five banking days after issuance unless redeemed beforehand or unless approval was given to extend that period.

324. Where an international customer used a personal cheque to draw down funds under a CCF, the cheque was banked no later than 20 banking days after issuance unless redeemed beforehand or approval was given to extend the period.

325. For the purposes of paragraphs 326 to 331, **CCF cheque** refers to a personal cheque, counter cheque, or a company cheque accepted by way of a substitution voucher.

326. A customer could redeem a CCF cheque by:

a. a cash payment at the Cage by the customer;

b. domestic or international telegraphic transfer to Crown Melbourne or Crown Perth by the customer;

c. domestic or international telegraphic transfer to Crown Melbourne or Crown Perth by a third party;

d. applying gaming chips, CPVs, or cash equivalents held by the customer;

e. transferring funds from the customer's DAB account;

f. a set-off of winnings by the customer at either Crown Melbourne or Crown Perth; or

g. other set-offs, as agreed.

Particulars

See the particulars at paragraph 219.

327. The banking or redemption of a CCF cheque (or the acceptance of a repayment under a CCF) was a transaction in relation to a loan where the loan was made in the course of carrying on a loans business.

Particulars

See the particulars at 313.

328. Crown Melbourne and Crown Perth provided an item 7, table 1, s6 designated service when it banked or redeemed a CCF cheque (or accepted repayment under a CCF).

Particulars

See paragraph 322.

329. If a cheque under a CCF was dishonoured, Crown Melbourne and Crown Perth would recover payment from the customer in other ways.

330. The recovery of funds owed under a CCF by Crown Melbourne and Crown Perth if a CCF cheque was dishonoured involved a transaction in relation to a loan where the loan was made in the course of carrying on a loans business.

Particulars

See the particulars at paragraph 313.

331. Crown Melbourne and Crown Perth provided an item 7, table 1, s6 designated service when it recovered funds owed under a CCF.

Particulars

See the matters pleaded at paragraph 322.

Overseas deposit services

332. Crown Melbourne and Crown Perth provided overseas deposit services to customers through:

a. the City of Dreams casino in Macau until May 2017;

b. the City of Dreams casino in Manila until May 2017;

c. Company 10, based in South East Asia, from at least 1 January 2015 until September 2020;

d. Crown Aspinalls in London at all times; and

e. Suncity junket desks that operated at various Macau casinos, including City of Dreams (the **Suncity deposit service**), as described at paragraph 423.

(the **overseas deposit services**).

333. The overseas deposit services were largely governed by practice and convention rather than under any documented process or procedures.

The City of Dreams deposit service

334. Prior to May 2017, Crown Resorts was a major shareholder in Melco Crown Entertainment Limited (later Melco Resorts & Entertainment Limited), which beneficially owned the City of Dreams in Macau and had a 68% to 73% interest in City of Dreams in Manila.

335. The deposit services provided by the City of Dreams at Macau and at City of Dreams Manila (together, the **City of Dreams**) each operated in the same way (the **City of Dreams deposit services**).

336. Crown Melbourne and Crown Perth understood that the City of Dreams deposit service in Macau and Manila were available only to mutual customers of any Crown casino and one of the City of Dreams properties.

337. A person (the **depositor**) could deposit funds at the City of Dreams Cage.

338. The depositor could deposit funds with the City of Dreams by way of cash, chips or in other forms (the **City of Dreams deposit**).

339. The City of Dreams deposit could be used for two purposes:

a. as security for a loan provided by Crown Melbourne or Crown Perth to a customer for play on a junket or Premium Player Program, as pleaded at paragraphs 344 to 358; or

b. to discharge a debt owed to Crown Melbourne or Crown Perth by a customer, in accordance with the procedure pleaded at paragraph 401.

340. Crown Melbourne and Crown Perth relied upon the City of Dreams to identify the depositor.

341. The City of Dreams Cage was required to collect identification documents (either a passport or country identification card), residential address and date of birth of the depositor.

342. There was no requirement or process in place to ensure that the depositor and the customer was the same person.

343. No source of funds checks were applied by Crown Melbourne, Crown Perth or City of Dreams with respect to either the depositor or the customer.

344. On receipt of a deposit:

a. The City of Dreams Cage would complete a Funds Collection Receipt (**FCR**) which contained the depositor's name, identification details, address, and the amount deposited.

b. The FCR also identified the customer to whom the funds should be made available.

c. Copies of the FCR were given to the depositor and sent via email by the City of Dreams Cage to the Crown Melbourne or Crown Perth Cage.

345. Funds were not made available to the Crown Melbourne or Crown Perth customer until:

a. the email pleaded at paragraph 344c had been received by Crown Melbourne or Crown Perth;

b. the customer presented at the Crown Melbourne or Crown Perth Cage;

c. the customer provided Crown Melbourne or Crown Perth with a copy of their identification for verification that it matched the customer name identified in the FCR;

d. the Crown Melbourne or Crown Perth customer signed the telegraphic transfer acknowledgment paperwork; and

e. an approval was obtained for the 'early release' of the funds to the Crown Melbourne or Crown Perth customer, generally by at least two authorised signatories.

346. For amounts exceeding $1 million, one of the signatories was required to have been a member of executive management.

347. The approved funds were credited to the Crown Melbourne or Crown Perth customer's DAB account.

Particulars

This was an item 13, table 3, s6 designated service.

348. The approval of the early release of funds by Crown Melbourne or Crown Perth to its customer involved the provision of a loan.

Particulars

Paragraphs (a) and/or (b) of the definition of 'loan' in s5 of the Act.

These loans are referred to at paragraphs 349 to 358 as **the loans** or **the loan**.

349. The City of Dreams deposit was held as security for the loan.

350. At all times, Crown Melbourne and Crown Perth provided the loans to their customers in the course of carrying on a loans business.

Particulars

The provision of loans to customers was a 'core activity' of the Crown Melbourne and Crown Perth businesses that facilitated the generation of gaming revenue.

See paragraphs 288 and 313.

The provision of loans involved systemisation and repetition.

The provision of loans facilitated the provision of table 3 s6 gaming services to a material number of high value customers.

351. At all times, the provision of the loans by Crown Melbourne and Crown Perth to its customers were item 6, table 1, s6 designated services.

Particulars

See paragraphs 348 and 349.

352. After approved funds were credited to a customer's DAB account, the customer could:

a. draw those funds out as a chip purchase voucher to obtain program chips. The program chips would then be used to facilitate item 6, table 3 designated services through a program; or

b. transfer some of those funds to another customer's DAB account in the following circumstances only:

i. Funds could be transferred to a person with whom the customer was associated. For example, a customer was permitted to transfer some of the funds to a spouse so the spouse could also play on the program or start a program in their own name; or

ii. A junket player could transfer some of the funds to a junket operator for use on the junket program; or

Particulars

Funds transferred as pleaded at 352b i or ii were used to facilitate item 6, table 3, s6 designated services through a program

c. cash out up to five percent of the approved funds, or up to a set cash out limit approved by Crown's VIP International senior management. The cash out was intended to be applied for a non-gaming purpose, such as towards shopping or holiday expenses during the customer's trip.

353. Where, at the conclusion of a program, a customer won more than the amount of the loan that was provided to them:

a. The Crown Melbourne or Crown Perth Cage would notify the City of Dreams Cage, who would make the deposit available for the original depositor to collect at the City of Dreams Cage.

b. The deposit could not be collected by anyone other than the depositor and had to be collected in the same form as it was deposited (for example, cash or chips).

c. The Crown Melbourne or Crown Perth Cage paid the customer the amount that was won over and above the amount of the loan it had provided to the customer. This was an item 9, table 3, s6 designated service.

d. The Crown Melbourne or Crown Perth Cage offset the amount owed by the customer under the loan against the customer's winnings and would use the offset to discharge the debt under the loan. The discharge of the debt was an item 7, table 1 designated services, for the reasons pleaded at paragraphs 357 to 358 below.

354. Subject to paragraph 356, where, at the conclusion of a program, a customer lost the full amount of the loan that was provided to them:

a. The Crown Melbourne or Crown Perth Cage would notify the City of Dreams Cage and provide evidence of the loss.

b. The City of Dreams Cage would transfer an amount equal to the City of Dream deposit from its bank account to Crown Melbourne's or Crown Perth's bank account.

c. On receipt of the funds, Crown Melbourne or Crown Perth would discharge the debt owed by its customer pursuant to the loan. The discharge of the debt was an item 7, table 1 designated services, for the reasons pleaded at paragraphs 357 to 358 below.

355. Subject to paragraph 356, where, at the conclusion of a program, a customer lost some, but not all, of the amount of the loan that was provided to them (a **partial loss**):

a. The Crown Melbourne or Crown Perth Cage would notify the City of Dreams Cage and provide evidence of the partial loss.

b. The City of Dreams Cage would then transfer an amount equal to the partial loss from its bank account to Crown Melbourne's or Crown Perth's bank account.

c. On receipt of the funds, Crown Melbourne or Crown Perth would discharge the debt owed by its customer pursuant to the loan. The discharge of the debt was an item 7, table 1 designated services, for the reasons pleaded at paragraphs 357 to 358 below.

356. A customer could repay an amount owed under the loan by means other than those pleaded at paragraphs 354 and 355 as follows:

a. The customer could make a payment to Crown Melbourne or Crown Perth by:

i. applying the proceeds of the customer's program by way of a credit to the customer's DAB account;

ii. telegraphic transfer; or

iii. bank draft

within three business days from departure from the casino after the program.

b. On receipt of the funds, Crown Melbourne or Crown Perth would discharge the debt owed by its customer pursuant to the loan. The discharge of the debt was an item 7, table 1 designated services, for the reasons pleaded at paragraphs 357 to 358 below.

c. Crown Melbourne or the Crown Perth would notify the City of Dreams Cage that the customer had discharged the loan.

d. The City of Dreams would make the City of Dreams deposit available for the original depositor to collect at the City of Dreams Cage.

e. The deposit could not be collected by anyone other than the depositor and had to be collected in the same form as it was deposited (for example, cash or chips).

357. The discharge of a debt owed under the loan involved a transaction in relation to a loan where the loan was made in the course of carrying on a loans business.

Particulars

See the particulars at paragraph 349.

358. Crown Melbourne and Crown Perth provided an item 7, table 1, s6 designated service when it discharged a debt owed under the loan.

Particulars

See paragraphs 353d, 354c, 355c and 356b.

The South East Asian deposit service offered by Company 10

359. From at least 1 January 2015 until September 2020, a company based in South East Asia (**Company 10**), operated a deposit service that was similar to the City of Dreams deposit service (the **Company 10 deposit service**).

360. Company 10 was money changer operated by an individual named Person 56. Person 56 was also the majority shareholder in Company 10. Person 56 was herself a customer of Crown Melbourne and Crown Perth, as well as a junket tour representative and key player with a junket at Crown Melbourne.

361. A person could deposit funds with Company 10 on behalf of a Crown Melbourne or Crown Perth customer for play on a junket or premium player program (the **deposit**).

362. Crown Melbourne and Crown Perth did not conduct identification, source of funds or wealth checks on the person who deposited the funds with Company 10.

363. Person 56 provided Crown Melbourne and Crown Perth with a letter confirming the amount that was held on behalf of a customer.

364. The deposit was held by Company 10 until the customer's play on the program had concluded.

365. In reliance upon this letter, Crown Melbourne or Crown Perth approved the early release of funds to its customer.

366. The approval of the early release of funds by Crown Melbourne or Crown Perth to its customer involved the provision of a loan.

Particulars

Paragraph (a) and/or (b) of the definition of 'loan' in s5 of the Act.

These loans are referred to at paragraphs 367 to 374 as **the loans** or **the loan**.

367. The deposit was security for the loan pleaded at paragraph 366.

368. At all times, Crown Melbourne and Crown Perth provided the loans to their customers in the course of carrying on a loans business.

Particulars

The provision of loans to customers was a 'core activity' of the Crown Melbourne and Crown Perth businesses that facilitated the generation of gaming revenue.

See the particulars at paragraphs 288, 313 and 350.

The provision of loans involved systemisation and repetition.

The provision of loans facilitated the provision of table 3 s6 gaming services to a material number of high value customers.

369. At all times, the provision of the loans by Crown Melbourne and Crown Perth to its customers were item 6, table 1, s6 designated services.

Particulars

See paragraphs 366 to 368.

370. Where, at the conclusion of a program, a customer won more than the amount of the loan that was provided to them:

a. The Crown Melbourne or Crown Perth Cage paid the customer the amount that was won over and above the amount of the loan it had provided to the customer. This was an item 9, table 3, s6 designated service.

b. The Crown Melbourne or Crown Perth Cage offset the amount owed by the customer under the loan against the customer's winnings and would use the offset to discharge

the debt under the loan. The discharge of the debt was an item 7, table 1 designated services, for the reasons pleaded at paragraphs 373 to 374 below.

371. Where, at the conclusion of a program, a customer lost the full amount of the loan that was provided to them:

a. The Crown Melbourne or Crown Perth Cage would notify Company 10 and provide evidence of the loss.

b. Company 10 would transfer an amount equal to the deposit from its bank account to Crown Melbourne's or Crown Perth's bank account.

c. On receipt of the funds, Crown Melbourne or Crown Perth would discharge the debt owed by its customer pursuant to the loan. The discharge of the debt was an item 7, table 1 designated services, for the reasons pleaded at paragraphs 373 to 374 below.

372. Where, at the conclusion of a program, a customer lost some, but not all, of the amount of the loan that was provided to them (a **partial loss**):

a. The Crown Melbourne or Crown Perth Cage would notify Company 10 and provide evidence of the partial loss.

b. Company 10 would then transfer an amount equal to the partial loss from its bank account to Crown Melbourne's or Crown Perth's bank account.

c. On receipt of the funds, Crown Melbourne or Crown Perth would discharge the debt owed by its customer pursuant to the loan. The discharge of the debt was an item 7, table 1 designated service, for the reasons pleaded at paragraphs 373 to 374 below.

373. The discharge of a debt owed under the loan involved a transaction in relation to a loan where the loan was made in the course of carrying on a loans business.

Particulars

See the particulars at paragraph 368.

374. Crown Melbourne and Crown Perth provided an item 7, table 1, s6 designated service when it discharged a debt owed under the loan.

Particulars

See paragraphs 370.b, 371c and 372c.

Crown Aspinalls London

375. A person could deposit funds in foreign currency with Crown Aspinalls London on behalf of a Crown Melbourne or Crown Perth customer for play on a junket or premium player program (the **Aspinalls deposit**).

376. There was no requirement that the person who deposited the funds be the same person as the Crown Melbourne or Crown Perth customer.

377. However, the funds deposited at Aspinalls were generally existing funds held on account at the Aspinalls Cage by a person who was seeking to:

a. use some or all of those funds for gaming at Crown Melbourne or Crown Perth; or

b. to repay a debt owed to Crown Melbourne or Crown Perth, as pleaded at paragraph 402.

378. When a customer deposited funds with Crown Aspinalls, the Cage staff at Crown Aspinalls:

a. applied identification checks to the depositor in accordance with their local AML requirements; and

b. sent an email to Crown Melbourne or Crown Perth to advise of the amount of funds received, details of the depositor, and copies of identification documents.

379. Funds were not made available to the Crown Melbourne or Crown Perth customer until:

a. the email pleaded at paragraph 378b had been received by Crown Melbourne or Crown Perth;

b. the customer presented at the Crown Melbourne or Crown Perth Cage;

c. the customer provided Crown Melbourne or Crown Perth with a copy of their identification for verification that it matched the customer name identified in the email;

d. the Crown Melbourne or Crown Perth customer signed the telegraphic transfer acknowledgment paperwork; and

e. an approval was obtained for the 'early release' of the funds to the Crown Melbourne or Crown Perth customer, generally by at least two authorised signatories.

380. For amounts exceeding $1 million, one of the signatories was required to have been a member of executive management.

381. The approved funds were credited to the Crown Melbourne or Crown Perth customer's DAB account.

Particulars

This was an item 13, table 3, s6 designated service.

382. The approval of the early release of funds by Crown Melbourne or Crown Perth to its customer involved the provision of a loan.

Particulars

Paragraph (a) and/or (b) of the definition of 'loan' in s5 of the Act.

These loans are referred to at paragraphs 383 to 392 as **the loans** or **the loan**.

383. The Aspinalls deposit was held as security for the loan.

384. At all times, Crown Melbourne and Crown Perth provided the loans to their customers in the course of carrying on a loans business.

Particulars

The provision of loans to customers was a 'core activity' of the Crown Melbourne and Crown Perth businesses that facilitated the generation of gaming revenue.

See the particulars at paragraphs 288, 313, 350 and 368.

The provision of loans involved systemisation and repetition.

The provision of loans facilitated the provision of table 3 s6 gaming services to a material number of high value customers.

385. At all times, the provision of the loans by Crown Melbourne and Crown Perth to its customers were item 6, table 1, s6 designated services.

Particulars

See paragraphs 382 and 384.

386. After approved funds were credited to a customer's DAB account, the customer could:

a. draw those funds out as a chip purchase voucher to obtain program chips. The program chips would then be used to facilitate item 6, table 3 designated services through a program; or

b. transfer some of those funds to another customer's DAB account in the following circumstances only:

i. Funds could be transferred to a person with whom the customer was associated. For example, a customer was permitted to transfer some of the funds to a spouse so the spouse could also play on the program or start a program in their own name; or

ii. A junket player could transfer some of the funds to a junket operator for use on the junket program.

iii. Funds transferred as pleaded at 386b i or ii were used to facilitate item 6, table 3 designated services through a program.

c. cash out up to five percent of the approved funds, or up to a set cash out limit approved by Crown's VIP International senior management. The cash out was intended to be applied for a non-gaming purpose, such as towards shopping or holiday expenses during the customer's trip.

387. Where, at the conclusion of a program, a customer won more than the amount of the loan that was provided to them:

a. The Crown Melbourne or Crown Perth Cage would notify the Aspinalls Cage, who would make the deposit available for the original depositor to collect at the City of Dreams Cage.

b. The Crown Melbourne or Crown Perth Cage paid the customer the amount that was won over and above the amount of the loan it had provided to the customer. This was an item 9, table 3, s6 designated service.

c. The Crown Melbourne or Crown Perth Cage offset the amount owed by the customer under the loan against the customer’s winnings and would use the offset to discharge the debt under the loan. The discharge of the debt was an item 7, table 1 designated service, for the reasons pleaded at paragraphs 391 to 392 below.

388. Subject to paragraph 390, where, at the conclusion of a program, a customer lost the full amount of the loan that was provided to them:

a. The Crown Melbourne or Crown Perth Cage would notify the Aspinalls and provide evidence of the loss.

b. The Aspinalls Cage would transfer an amount equal to the Aspinalls deposit from its bank account to Crown Melbourne’s or Crown Perth’s bank account.

c. On receipt of the funds, Crown Melbourne or Crown Perth would discharge the debt owed by its customer pursuant to the loan. The discharge of the debt was an item 7, table 1 designated service, for the reasons pleaded at paragraphs 391 to 392 below.

389. Subject to paragraph 390, where, at the conclusion of a program, a customer lost some, but not all, of the amount of the loan that was provided to them (a **partial loss**):

a. The Crown Melbourne or Crown Perth Cage would notify the Aspinalls Cage and provide evidence of the partial loss.

b. The Aspinalls Cage would then transfer an amount equal to the partial loss from its bank account to Crown Melbourne's or Crown Perth's bank account.

c. On receipt of the funds, Crown Melbourne or Crown Perth would discharge the debt owed by its customer pursuant to the loan. The discharge of the debt was an item 7, table 1 designated service, for the reasons pleaded at paragraphs 391 to 392 below.

390. A customer could repay an amount owed under the loan by means other than those pleaded at paragraphs 388 and 389 as follows:

a. The customer could make a payment to Crown Melbourne or Crown Perth by:

i. applying the proceeds of the customer's program by way of a credit to the customer's DAB account;

ii. telegraphic transfer; or

iii. bank draft

within three business days from departure from the casino after the program.

b. On receipt of the funds, Crown Melbourne or Crown Perth would discharge the debt owed by its customer pursuant to the loan. The discharge of the debt was an item 7, table 1 designated services, for the reasons pleaded at paragraphs 391 to 392 below.

c. Crown Melbourne or Crown Perth would notify the Aspinalls Cage that the customer had discharged the loan.

d. The Aspinalls Cage would make the Aspinalls deposit available for the original depositor to collect at the Aspinalls Cage.

e. The deposit could not be collected by anyone other than the depositor and had to be collected in the same form as it was deposited (for example, cash or chips).

391. The discharge of a debt owed under the loan involved a transaction in relation to a loan where the loan was made in the course of carrying on a loans business.

Particulars

See the particulars at paragraph 384.

392. Crown Melbourne and Crown Perth provided an item 7, table 1, s6 designated service when it discharged a debt owed under the loan.

Particulars

See paragraphs 387c, 388c, 389c and 390b.

ML/TF risk assessments of credit facilities, CCFs and overseas deposit services

393. At no time did Crown Melbourne or Crown Perth carry out an ML/TF risk assessment of the item 6 and 7, table 1, s6 designated services provided through:

a. credit facilities;

b. CCFs; or

c. overseas deposit services.

394. The provision of item 6 and 7, table 1, s6 designated services by Crown Melbourne and Crown Perth through credit facilities, CCFs and overseas deposit services involved higher ML/TF risks:

a. Loans under credit facilities, CCFs and overseas deposit services could be drawn down and repaid as part of a complex chain of different designated services under tables 1 and 3, s6 of the Act.

b. Credit facilities, CCFs and overseas deposit services enabled funds held by customers in foreign jurisdictions to be used in Australia without the need for a cross-border transfer.

c. Loans under credit facilities, CCFs and overseas deposit services could be drawn down by way of DAB account deposit and then withdrawn in cash.

d. Loans under credit facilities, CCFs and overseas deposit services could be repaid through non-face-to-face channels, including by international and domestic telegraphic transfers.

e. Loans under credit facilities and CCFs and overseas deposit services could be repaid by third party transfers through non-face-to-face channels, including third party companies, through overseas deposit services and by foreign money remitters.

Particulars

See the particulars at paragraph 219.

f. Loans under overseas deposit services could be repaid by third party transfers through non-face-to-face channels, including third party companies and by foreign money remitters.

Particulars

See the particulars at paragraph 219.

g. Crown Melbourne and Crown Perth could issue a substitution voucher to replace a credit marker or counter cheque with a personal or company cheque for the same value.

h. At Crown Melbourne, a counter cheque could be issued at a gaming table location, as well as at the Cage.

i. Crown Melbourne and Crown Perth customers accessing funds via an overseas deposit service did not need to be the same person as the depositor.

j. Company 10, who offered the overseas deposit service in South East Asia, was also a remitter and a junket operator.

k. The provision of loans via credit facilities, CCFs and overseas deposit services by Crown Melbourne and Crown Perth created an avenue for money laundering through smurfing or cuckoo smurfing.

l. Junkets operators and representatives were provided with significant lines of credit through credit facilities and CCFs. Following each drawdown of a credit facility or CCF by the junket operator or junket representative, chip purchase vouchers, gaming chips or cash equivalents that were issued by Crown Melbourne or Crown Perth would be provided at the junket operator's or representative's discretion to the junket players.

Particulars

See paragraph 487.

m. Credit facilities could be shared across Crown Melbourne and Crown Perth.

The Part A Programs did not apply controls to loans - credit facilities, CCFs and overseas deposit services

395. The Standard Part A Programs did not apply to item 6 and 7, table 1, s6 designated services and were not capable, by design, of identifying, mitigating and managing the ML/TF risks of these designated services.

a. The Standard Part A Programs did not include systems and controls to ensure that the approval of loans had regard to ML/TF risks.

b. The approval of credit limits under credit facilities and CCFs was subject to credit risk assessments not ML/TF risk assessments.

c. The approval of the ‘early release of funds’ under overseas deposit services did not have regard to ML/TF risk assessments.

d. The Standard Part A Programs did not include appropriate preventative controls to mitigate and manage the ML/TF risks of loans and loan repayments, such as controls to:

i. impose limits on credit;

ii. identify customers to whom the provision of credit was outside of risk appetite;

iii. restrict the ability of third parties to repay loans on behalf of customers.

e. The Standard Part A Programs did not include controls to monitor drawdowns under credit facilities and CCFs.

f. The Standard Part A Programs did not have any processes in place to identify how, for example, the gaming chips issued by Crown, based on the approved junket credit, were subsequently distributed among the junket players by the junket operator or representative.

g. The Standard Part A Programs did not include any controls requiring the customer accessing funds via an overseas deposit service to be the same person as the depositor; nor did they include controls for Crown Melbourne or Crown Perth to verify that the depositor and customer were the same person.

Particulars

By no later than June 2018, the Chief Legal officer of Crown Resorts, who was also the AMLCO for both Crown Melbourne and Crown Perth was briefed on a recommendation from the Group General Manager AML (Melbourne) that Crown's credit policies and the means of repayment from offshore be taken to the Board for its consideration as to its comfort level.

The Group General Manager AML also recommended that a compliance review be conducted on all credit arrangements.

This compliance review did not occur and did not prompt any review of AML/CTF requirements with respect to credit facilities, CCFs and overseas deposit services.

See the particulars at paragraph 219.

Remittance services - items 31 and 32 table 1, s6 designated services

396. The Standard Part A Programs did not include appropriate risk-based systems and controls that were capable by design of identifying, mitigating and managing the ML/TF risks reasonably faced by Crown Melbourne and Crown Perth with respect to item 31 and 32, table 1, s6 designated services (**remittance services**) for the reasons pleaded at paragraphs 397 to 423 below.

397. Crown Melbourne and Crown Perth were non-financiers.

Particulars

Section 5 of the Act.

Item 32, table 1, s6 designated services - deposits into Crown bank accounts

398. At all times, a customer could deposit money, or arrange for money to be deposited into a Crown Melbourne or Crown Perth bank account (including Crown Patron accounts) to:

a. transfer front money for a visit to the casino; or

b. transfer funds from another casino, including an Australian or foreign casino.

399. At all times, in each circumstance identified in paragraph 398, Crown Melbourne or Crown Perth made the deposited money available to the customer by crediting the money to the customer's DAB account.

400. At all times, a customer could deposit money, or arrange for money to be deposited into a Crown Melbourne or Crown Perth bank account (including Crown Patron accounts) to repay an amount owed to Crown Melbourne or Crown Perth under a loan, including:

a. through the City of Dreams deposit service, as described at paragraph 401 below;

b. through the Aspinalls London deposit service, as described at paragraph 402 below; or

c. otherwise, by telegraphic transfer or cash deposit.

401. Until May 2017, a customer could arrange for any debt owed to Crown Melbourne or Crown Perth to be repaid through the City of Dreams Deposit service, in accordance with the following process:

a. A person could deposit funds with the City of Dreams.

b. The depositor was required to notify the City of Dreams that the deposit was being made to repay a debt owed to Crown Melbourne or Crown Perth by a customer.

c. There was no processes in place to require or check that the depositor and customer were the same person.

d. The Cage team at the City of Dreams casino would then send the Crown Melbourne Cage or Crown Perth Cage a receipt that included details of the depositor's name, address, identification details, and an image of the identification document.

e. The Crown Melbourne Cage or Crown Perth Cage would then verify the debt owed by the Crown Melbourne or Crown Perth customer and provide the Cage team at the City of Dreams with evidence of the customer's debt.

f. Following this verification process, the funds would then be transferred from a City of Dreams bank account to one of Crown Melbourne's or Crown Perth's bank accounts in full or partial satisfaction of the debt owed by the customer to Crown Melbourne or Crown Perth.

402. At all times, funds held on account with Crown Aspinalls could be applied to discharge a debt owed by a customer of Crown Melbourne or Crown Perth. In these circumstances, Crown Aspinalls would deposit funds into a Crown Melbourne bank or Crown Perth bank account by way of telegraphic transfer.

403. At all times, in each circumstance identified in paragraph 400, Crown Melbourne or Crown Perth made the deposited money available to the customer by redeeming the debt:

a. through an entry on the customer's DAB account to reflect the amount repaid.

b. through the redemption screen on SYCO, which sat separately to a customer's DAB account on SYCO, to reflect the amount paid.

404. At all times, with respect to each of the transactions pleaded at paragraphs 399 and 403, Crown Melbourne and Crown Perth made money available, or arranged for it to be made available to customers as a result of transfers under a designated remittance arrangement.

405. At all times, Crown Melbourne and Crown Perth provided the services as described at paragraph 404 in the course of carrying on a business of giving effect to remittance arrangements.

Particulars

The provision of remittance services was a 'core activity' of the Crown Melbourne and Crown Perth businesses.

The provision of remittance services involved systemisation and repetition.

The provision of remittance services facilitated table 3, s6 designated services and therefore facilitated the generation of gaming revenue.

406. At all times, Crown Melbourne and Crown Perth provided designated services within the meaning of item 32, table 1, s6 when it provided the services described at paragraph 404.

Item 31, table 1, s6 designated services - transfers from DAB accounts via Crown bank accounts

407. At all times, a customer could instruct Crown Melbourne or Crown Perth to transfer money via telegraphic transfer from their DAB account or safekeeping account to:

a. a bank account - either in the customer's name or a third party's name - for the purposes of returning front money or remitting winnings; or

b. another casino, including an Australian or foreign casino.

Particulars

See the particulars at paragraph 219.

408. At all times, with respect to each of the transfers pleaded at paragraph 407, Crown Melbourne and Crown Perth accepted instructions from the customer for the transfer of money under a designated remittance arrangement.

409. At all times, Crown Melbourne and Crown Perth provided the services as described at paragraph 408 in the course of carrying on a business of giving effect to remittance arrangements.

Particulars

See paragraph 405.

410. At all times, Crown Melbourne and Crown Perth provided designated services within the meaning of item 31, table 1, s6 when it provided the services described at paragraph 408.

Items 31 and 32, table 1, s6 designated services - transfers between DAB accounts

411. At all times, Crown Melbourne or Crown Perth could transfer money from one customer's DAB account (the **first customer**) to another customer's DAB account (the **second customer**) at the first customer's request.

412. At all times, when Crown Melbourne and Crown Perth transferred money from the first customer's DAB account to the second customer's DAB account, Crown Melbourne or Crown Perth:

a. accepted instructions from the first customer for the transfer of money under a designated remittance arrangement; and

b. made money available, or arranged for it to be made available to the second customer as a result of transfers under a designated remittance arrangement.

413. At all times, Crown Melbourne and Crown Perth provided the services as described at paragraph 412 in the course of carrying on a business of giving effect to remittance arrangements.

Particulars

See paragraph 405.

414. At all times, Crown Melbourne and Crown Perth provided designated services within the meaning of item 31, table 1, s6 when it provided the services described at paragraph 412a.

415. At all times, Crown Melbourne and Crown Perth provided designated services within the meaning of item 32, table 1, s6 when it provided the services described at paragraph 412b.

Item 32, table 1, s6 designated services - the HCT channel

416. At all times prior to October 2016, Crown Melbourne made money available to customers through the HCT channel as described in paragraph 244 above.

417. Crown Melbourne made the money available to the customer through the HCT channel by:

a. entering a credit on to the customer's DAB account; or

b. issuing the customer with a CEV.

418. At all times, Crown Melbourne and Crown Perth provided the services as described at paragraph 417 in the course of carrying on a business of giving effect to remittance arrangements.

Particulars

See paragraph 405.

419. At all times, Crown Melbourne and Crown Perth provided designated services within the meaning of item 32, table 1, s6 when it provided the services described at paragraph 417.

ML/TF risk assessments of items 31 and 32, table 1, s6 designated services

420. Items 31 and 32 table 1, s6 remittance services provided by Crown Melbourne and Crown Perth involved higher ML/TF risks because:

a. Money could be remitted 24 hours a day 7 days a week, including offshore.

b. Remittance services were often provided as part of a complex chain of different designated services under tables 1 and 3, s6 of the Act.

c. There were no transaction limits on telegraphic transfers into or out of a DAB account or safekeeping account.

d. There were no transaction limits on transfers between DAB accounts.

e. Remittance services were facilitated through Crown Patron accounts, including the Southbank accounts and Riverbank accounts, which lacked transparency and over which Crown had limited visibility.

f. Remittance services were facilitated through the HCT channel, which lacked transparency and involved customers with a jurisdictional profile involving higher ML/TF risks.

g. Remittance services were facilitated through overseas deposit services, including through the City of Dreams service, which lacked transparency and over which Crown had limited visibility.

h. Money could be transferred to and from bank accounts (both domestic and foreign).

i. Money could be transferred to and from other casinos, including offshore casinos.

j. Money could also be transferred to and from other customers' DAB accounts and safekeeping accounts.

k. Funds could be made available to third parties through remittance services, where Crown Melbourne or Crown Perth had limited or no understanding of who the third party was.

l. A customer's debt to Crown Melbourne or Crown Perth could be settled by a third party through remittance services, where Crown Melbourne or Crown Perth had limited or no understanding of who the third party was or their source of funds.

m. Remittance services were not conducted face-to-face where Crown Melbourne and Crown Perth facilitated the transfer of funds via electronic transfers (including telegraphic transfer, IFTIs, internet transfers and direct deposit).

n. Crown Melbourne and Crown Perth would assist junket operators to distribute winnings to individual junket players:

i. This would be done by transferring funds from the DAB account of a junket operator to the DAB account of a junket player, as well as transferring funds from a junket operator's DAB account by telegraphic transfer to a junket player.

ii. Crown Melbourne had very limited or no visibility over how winnings were attributed to junket players or how the junket operator funded their front money.

o. Crown Melbourne and Crown Perth provided items 31 and 32 table 1, s6 designated services in Australian dollars and foreign currencies.

Particulars

See the particulars at paragraph 219.

421. At no time did Crown Melbourne or Crown Perth carry out an appropriate ML/TF risk assessment of items 31 and 32 table 1, s6 designated services.

422. From 1 March 2016 to 1 November 2020, the Standard Part A Programs did not include appropriate risk-based systems and controls that were capable by design of identifying, mitigating and managing the ML/TF risks reasonably faced by Crown Melbourne or Crown Perth with respect to items 31 and 32, table 1, s6 designated services for the following reasons:

a. The Standard Part A Programs did not include appropriate risk-based controls that were aligned and proportionate to the higher ML/TF risks identified at paragraph 420.

b. No appropriate preventative controls were applied to remittance services to mitigate and manage ML/TF risks, such as controls to:

i. restrict remittance to and from third parties;

ii. require senior management approval of remittance at or above appropriate pre-determined levels, with the criteria for approval having regard to ML/TF risks; and/or

iii. impose daily or transaction limits on remittance.

Particulars

See the particulars at paragraph 219.

423. At no time did Crown Melbourne or Crown Perth consider or assess the ML/TF risks of providing item 31 and 32, table 1, s6 designated services through the Suncity deposit service channel, before this channel was adopted.

a. In May 2017, a Crown Resorts employee opened an account in his personal name with Suncity in Macau (the **Suncity account**).

b. The account, being in the personal name of an individual employee, had no transparency.

c. The Suncity account was intended to be used to receive debt repayments to Crown Melbourne, Crown Perth and Crown Aspinalls.

d. Funds were to be remitted through this channel and made available by Crown Melbourne or Crown Perth to the customer by deposit to their DAB accounts (item 32, table 1, s6).

e. The VIP Finance team maintained a log of funds held in the Suncity account.

f. Shortly after the Suncity Account arrangements were put in place, Crown revisited its decision to offer this deposit service due to 'local AML concerns' identified by the Chief Legal Officer of Crown Resorts and AMLCO for both Crown Melbourne and Crown Perth.

g. However, in June 2017, Crown Melbourne agreed to process transactions through this service to settle an AUD$9.6 million debt owed to Crown Melbourne by a former customer (Customer 27), who had been excluded from the casino 8 years earlier as a result of criminal activity and concerns over source of wealth.

h. In June 2017 Customer 27 deposited HKD$4.8 million in cash into the Suncity account.

i. In April 2018 Crown Melbourne agreed to offset the HKD$4.8 million deposited by Customer 27 against 'lucky money' owed to the Suncity junket operator, Customer 1.

j. In May 2018, the SYCO record was updated to record that the customer's debt to Crown Melbourne had been discharged and that Crown Melbourne's debt to the junket operator had been discharged.

    i. The stop code on Customer 27's DAB account was lifted to enable the debt he owed to Crown Melbourne to be repaid. This was an item 32, table 1, s6 designated service and an item 13, table 1, s6 designated service.

    ii. Crown Melbourne also provided an item 32, table 1, s6 designated service by making the 'lucky money' available to Customer 1.

k. At all times, Crown Melbourne was aware that Customer 1 posed high ML/TF risks, by reason of alleged links to organised crime.

l. The Suncity deposit service channel had no transparency.

m. The ML/TF risks of facilitating designated services through this channel were not the subject of any ML/TF risk assessment before the Suncity account was opened.

n. The ML/TF risks of the designated services facilitated through this channel in May 2018 were not assessed.

Particulars

Rule 8.1.5(5)(b) of the Rules.

By no later than June 2018, the Chief Legal Officer of Crown Resorts, who was also the AMLCO for both Crown Melbourne and Crown Perth, was advised by the Group General Manager AML (Crown Melbourne) that the Suncity account remained open and had a balance in the order of $25 million. These deposits were described as being held 'ostensibly to repay debts owed to Crown'. In the briefing to the Chief Legal Officer/AMLCO, the Group General Manager expressed the concern that 'Crown had no clarity as to the source of these funds (only that they are not from winnings and are not front monies)'.

Exchanging money for casino value instruments, including chips and tokens (and vice-versa)

424. From 1 March 2016 to 1 November 2020, the Standard Part A Programs did not include appropriate risk-based systems and controls that were capable by design of identifying, mitigating and managing the ML/TF risks reasonably faced by Crown Melbourne and Crown Perth with respect to item 7 and 8, table 3, s6 designated services for the reasons pleaded at paragraphs 425 to 428 below.

425. Customers could use a number of different casino value instruments (**CVIs)** to obtain table 3, s6 designated services from Crown Melbourne and Crown Perth, including those pleaded below:

a. Chips:

i. The exchange of money for chips was an item 7, table 3, s6 designated service;

ii. The exchange of chips for money was an item 8, table 3, s6 designated service;

iii. Chips could be used to enter into a game within the meaning of item 6, table 3, s6;

iv. A customer could be paid chips as winnings for the purposes of item 9, table 3, s6.

b. Chip purchase vouchers (**CPVs**):

i. This was a voucher drawn on a customer's DAB account, which involved an item 13, table 3, s6 designated service.

ii. A CPV could be exchanged for gaming chips at a table or selected Cage locations.

iii. A customer could deposit funds held in a CPV into a DAB, which involved an item 13, table 3, s6 designated service.

iv. A CPV was a channel through which item 6 and 7 table 3, s6 designated services could be obtained.

c. Chip exchange vouchers (**CEVs**):

i. This was a document used by a customer who did not have a DAB account, but who wished to exchange cash for gaming chips.

ii. The CEV could be exchanged for gaming chips at a table.

iii. From 1 March 2016 to October 2016, a customer was able to redeem a HCT credit for a CEV as recorded against a customer's membership number.

iv. A CEV obtained with a HCT credit could be exchanged at the Cage for chips.

v. A CEV was a channel through which item 6 and 7 table 3, s6 designated services could be obtained.

d. 'Ticket in ticket out' tickets (**TITO tickets**)

i. A TITO ticket was a barcoded ticket dispensed from gaming machines when a customer elected to cash-out or won a jackpot.

ii. A TITO was a token.

iii. A customer received an item 9, table 3 s6 designated service when a TITO was dispensed from a gaming machine.

iv. A TITO ticket could be redeemed at the Cage or at a ticket redemption machine or **TRT**.

v. The redemption of a TITO ticket was an item 8, table 3, s6 designated service.

vi. A TITO ticket could be used again to obtain an item 6, table 3 s6 designated service on an electronic gaming machine or electronic gaming table.

vii. At Crown Melbourne, a TITO ticket could also be purchased at the Cage and used for gaming purposes.

viii. The purchase of a TITO ticket was an item 7, table 3, s6 designated service.

e. Hand-pay slips:

i. A hand pay slip was a manual ticket that was issued when a customer wanted to cash-out.

ii. A hand slip was used when TITO tickets were unable to be dispensed or where a customer won a jackpot.

iii. The issue of a hand-pay slip was an item 9, table 3, s6 designated service.

f. Prize certificates:

i. This was a certificate that represented value and was given to a customer to pay them for a prize they had won in a tournament or at a dinner event.

ii. The issue of a prize certificate was an item 9, table 3, s6 designated service insofar as it was won in a tournament.

iii. A prize certificate could be redeemed at the Cage.

g. Gaming chip vouchers:

i. This was a complimentary bet voucher that was issued to a customer.

ii. A gaming chip voucher could be exchanged for chips at a table.

iii. A gaming chip voucher was a channel through which item 6, table 3 s6 designated services could be obtained.

h. Crown Dollars:

i. This was a voucher that could be purchased from Crown Perth, only, that could be redeemed for chips, cash and Keno tickets.

ii. The purchase of Crown Dollars was an item 7, table 3, s6 designated service.

iii. The redemption of Crown Dollars for cash was an item 8, table 3, s6 designated service.

iv. Crown Dollars were a channel through which item 6, table 3, s6 designated services could be obtained.

426. The use of CVIs to obtain table 3, s6 designated services from Crown Melbourne and Crown Perth involved the following ML/TF higher risks:

a. Each of the above CVIs either directly involved the provision of table 3 designated services or were a channel through which table 3 designated services were provided.

b. During a visit to the casino, a customer could use CVIs to undertake multiple transactions, such as buying into and cashing out of table games or EGMs (items 6 and 9 table 3, s6), or transacting on a DAB account (item 13, table 3, s6).

c. Each of the above CVIs were highly transferrable and could be issued in large values.

d. Customers could therefore transfer value from one person to another by passing on the CVIs.

e. CVIs could not always be traced to an account holder or identified customer.

f. The redemption of CVIs could not always be attributable to winnings and could be cashed out with minimal or no play.

g. The issue or redemption of tickets was not always face-to-face.

h. In November 2016, Crown Melbourne approved an increase to the amount that was to be printed on tickets without human intervention of up to:

   i. $20,000 for restricted EGMs;

   ii. $20,000 for unrestricted EGMs and ETGs outside the Mahogany Room; and

   iii. $75,000 for unrestricted EGMs and ETGs within the Mahogany Room.

i. In November 2016, Crown Melbourne also approved the introduction of a facility for customers to purchase tickets directly from the Cage in premium areas, up to a maximum amount of $20,000.

j. Item 7, table 3 s6 designated services provided through the HCT channel involved higher ML/TF risks due to the HCT channel's lack of transparency and the jurisdictional profile of the customers using it.

k. By reason of a. to j., CVIs could be used to layer funds, as part of a more complex transaction chain of designated services, making it difficult to understand the purpose of transactions, the beneficial owner of funds or the ultimate beneficiary of value moved.

Particulars

Chapter 2 FATF/APG Casino Typologies Report.

See paragraph 24.

427. At no time did Crown Melbourne or Crown Perth conduct an appropriate ML/TF risk assessment of the provision of table 3, s6 gaming services through CVIs.

Particulars

Whilst the Risk Registers referred to some risks relating to CVIs, at no time did Crown Melbourne or Crown Perth adequately identify and assess all of the risks pleaded at paragraph 426.

At no time did Crown Melbourne or Crown Perth identify and assess the different ML/TF risks of different CVIs in accordance with an appropriate ML/TF risk methodology.

428. At no time did the Standard Part A Programs include appropriate risk-based systems and controls to identify, mitigate and manage the ML/TF risks of the provision of table 3 gaming services through CVIs:

a. At no time did the Standard Part A Programs include appropriate risk-based controls to mitigate and manage the ML/TF risks pleaded at paragraph 426.

b. With the exception of some limits on amounts printed on TITOs and transaction limits on TRTs, controls on CVIs were predominantly detective, not preventative. For the reasons pleaded at paragraph 433, the limits on TITO tickets posed ML/TF concerns.

c. Cage staff applying detective controls to item 8, table 3, s6 designated services did not have adequate visibility over these multiple transactions.

Table games and electronic gaming machines

429. From 1 March 2016 to 1 November 2020, the Standard Part A Programs did not include appropriate risk-based systems and controls that were capable by design of identifying, mitigating and managing the ML/TF risks reasonably faced by Crown Melbourne and Crown Perth with respect to item 6 and 9, table 3, s6 designated services for the reasons pleaded at paragraphs 430 to 435 below.

430. Crown Melbourne and Crown Perth provided designated services under items 6 and 9, table 3, s6 through:

a. table games; and

b. electronic gaming machines (**EGMs**), or pokie machines.

431. Crown Melbourne and Crown Perth offered a range of different table games.

a. Table games included roulette, baccarat, blackjack and poker.

b. Some table games were semi-automated or fully automated (electronic table games or **ETGs**).

432. Different table games and EGMs have different ML/TF risk profiles depending upon matters including:

a. whether they are face-to-face or not;

b. whether they permit even-money betting;

c. the degree of uncertainty of outcomes;

d. how rapidly money can be processed;

e. ticket limits, which can vary between machines;

f. whether they permit peer-to-peer gaming.

433. Table games and EGMs offered by Crown Melbourne and Crown Perth involved the following ML/TF risks:

a. Money could be moved through table games and EGMs through buying-in and cashing-out using cash, chips, TITO tickets and other CVIs.

b. Chips, TITOs and other CVIs were highly transferrable.

c. Customers could therefore transfer value from one person to another by passing on chips, TITOs, jackpot tickets and other CVIs.

d. EGMs and ETGs were not face-to-face.

e. Semi-automated table games involved less oversight by Crown Melbourne and Crown Perth staff.

f. Tickets from ETGs and EGMs could be issued in high values.

   i. From November 2016, the value of tickets that could be collected by a customer from a machine without human intervention increased from a $2,000 limit to:

      A. up to $20,000 (for restricted gaming machines and unrestricted gaming machines and ETGs outside of the Mahogany Room); and

      B. $75,000 (for unrestricted gaming machines and ETGs within the Mahogany Room).

g. Money including cash could be inserted into ETGs and EGMs, and tickets could be collected with minimal or no play up to the thresholds pleaded at f.

h. In table games that permit even-money wagering (such as roulette and baccarat), two customers could cover both sides of an even bet to give the appearance of legitimate gaming activity while minimising net losses.

i. Further, table games such as baccarat involve a low 'house edge'. Each hand can be high in value and is played within seconds. Money can therefore be turned-over very quickly, with minimal net loss and in collusion with other players.

j. The risks of even-money waging are higher with semi-automated and fully-automated games, as there is little to no oversight and a player can play several terminals at the same time.

k. EGMs and ETGS are vulnerable to refining because they process large volumes of smaller amounts quickly.

l. EGMs and ETGs are vulnerable to structuring and structured funds of $2,000 or under could be redeemed at non-face-to-face TRTs.

m. Card Play Extra credits, including credits derived from cash deposits, could be moved through EGMs: see paragraph 264 above.

n. Poker permitted peer-to-peer gaming, which posed risks of collusion.

o. Poker, particularly poker tournaments, could be used as a vehicle to legitimise the transfer of large amounts of funds between players.

p. By reason of a. to o., play on table games and EGMs could be used to layer funds, as part of a more complex transaction chain of designated services, making it difficult to understand the purpose of transactions, the beneficial owner of funds or the ultimate beneficiary of value moved.

Particulars

By no later than June 2018, the Chief Legal Officer of Crown Resorts, who was also the AMLCO for both Crown Melbourne and Crown Perth, was advised by the Group General Manager AML (Crown Melbourne) of AML concerns relating to the increase in the amount

printed on tickets as pleaded at g. and f. The Group General Manager AML recommended that the limit to be printed on tickets be reduced to below $10,000. In the absence of this change, the Group General Manager AML recommended that this limit be taken to the Board for consideration of its level of comfort.

See paragraph 24.

434. At no time did Crown Melbourne or Crown Perth identify and assess the different ML/TF risks of different table games and EGMs in accordance with an appropriate ML/TF risk methodology.

Particulars

See paragraphs 432 and 433.

435. At no time did the Standard Part A Programs include appropriate systems and controls to identify, mitigate and manage the ML/TF risks of designated services provided under items 6 and 9, table 3, s6 through each of the different table games and EGMs:

a. The Standard Part A Programs did not have appropriate regard to the different ML/TF risk profiles of different table games and EGMs when determining and putting in place risk-based systems and controls for items 6 and 9, table 3, s6 designated services.

b. The Standard Part A Programs did not include appropriate preventative controls, such as appropriate transaction or daily limits, with respect to buy-ins and cash-outs.

c. The Standard Part A Programs did not include appropriate risk-based procedures to understand source of wealth or funds with respect to item 6 and 9 table 3, s6 designated services (especially with respect to uncarded play as defined in paragraph 619).

d. Detective controls were largely reliant on staff observation and surveillance, which were inadequate including for the following reasons:

i. The ML/TF risks of EGMs and ETGs could not be adequately monitored by manual and observational methods;

ii. Manual and observational controls were not capable of consistently detecting the use of table games and EGMs to layer funds, as part of a more complex transaction chain of designated services; and

iii. The Part A detective controls did not allow the Cage visibility over any unusual patterns of activity on table games and EGMs at the point in time when the Cage exchanged chips, TITO tickets or other CVIs for money.

Foreign currency exchange - item 14, table 3, s6 designated services

436. From 1 March 2016 to 1 November 2020, the Standard Part A Programs did not include appropriate risk-based systems and controls that were capable by design of identifying, mitigating and managing the ML/TF risks reasonably faced by Crown Melbourne and Crown Perth with respect to item 14, table 1, s6 designated services for the reasons pleaded at paragraphs 437 to 442 below.

437. At all times, Crown Melbourne and Crown Perth provided foreign currency exchange services to customers within the meaning of item 14, table 3, s6 of the Act.

438. The Crown Melbourne and Crown Perth Cage each accepted physical currency, foreign drafts and travellers' cheques for the purposes of currency exchange.

439. Customers could also deposit or transfer funds into foreign currency accounts held by Crown. Crown would convert the funds to Australian dollars and make them available to the customer in their DAB account.

440. Currency exchange was also facilitated for customers who were repaying debts owed to Crown Melbourne and Crown Perth.

441. At no time did Crown Melbourne or Crown Perth carry out an ML/TF risk assessment with respect to designated services provided through its foreign currency accounts, including currency exchange services.

442. The Standard Part A Programs did not include appropriate risk-based systems and controls that were capable by design of identifying, mitigating and managing the ML/TF risks reasonably faced by Crown Melbourne and Crown Perth with respect to item 14, table 3, s6 designated services.

a. The FATF/APG Casino Typologies Report, Chapter 2, identifies indicators of money laundering using currency exchange, including:

i. bank drafts/cheques cashed in for foreign currency;

ii. multiple currency exchanges;

iii. dramatic or rapid increases in size and frequency of currency exchange transactions for regular account holders;

iv. currency exchange for no reasonable purpose;

v. currency exchanges with low denomination bills for high denomination bills;

vi. currency exchanges carried out by third parties;

vii. large, one-off, or frequent currency exchanges for customers not known to the casino;

viii. requests for casino cheques from foreign currency; and

ix. currency exchanges with little or no gambling activity.

b. The Standard Part A Programs did not include controls for monitoring transactions indicative of the above typologies.

Particulars

The Standard Part A Programs provided for yearly checks for foreign currency exchange to review any customers who have what appears to be an excessive number of foreign exchange transactions. This review was too infrequent and provided no criteria for review as against the typologies at a.

The Standard Part A Programs provided for some manual and observational controls with respect to 'Exchange of Foreign Currency – Exchange of small denomination notes to large denomination notes' and 'Exchange of Foreign Currency – inconsistent with any rated play', but did not provide any criteria for review.

c. The Standard Part A Programs did not include controls for monitoring transactions that did not involve the physical exchange of currency, such as transactions on DAB accounts involving foreign currency exchange, or the repayment of debts in foreign currency.

Designated services provided in foreign currencies

443. From 1 March 2016 to 1 November 2020, the Standard Part A Programs did not include appropriate risk-based systems and controls that were capable by design of identifying, mitigating and managing the ML/TF risks reasonably faced by Crown Melbourne and Crown Perth with respect to table 1 and table 3, s6 designated services provided in foreign currencies for the reasons pleaded at paragraphs 444 to 447 below.

444. At all times, Crown Melbourne and Crown Perth provided the following designated services in Hong Kong Dollars (**HKD**):

a. Table 3, s6 gaming services were provided to international program and junket players in HKD (with the exception of designated services provided through EGMs).

b. Crown Melbourne and Crown Perth issued chips in HKD, being item 7, table 3, s6 designated services.

c. Chips in HKD enabled customers to purchase table 3, s6 designated services in HKD.

d. Credit was provided to international program and junket players in HKD, involving item 6 and 7, table 1, s6 designated services.

e. Crown Melbourne and Crown Perth provided item 14, table 3, s6 designated services (currency exchange) in HKD to all customers.

445. From time to time, Crown Melbourne and Crown Perth also approved the provision of item 6 and 9, table 3, s6 designated services in other foreign currencies, in which case the table would be configured with the alternative currency in SYCO.

446. At no time did Crown Melbourne or Crown Perth conduct an assessment of the ML/TF risks of providing designated services in HKD and other foreign currencies.

447. At no time did the Standard Part A Programs have regard to the fact that some table 1 and table 3, s6 designated services were provided in HKD for the purposes of identifying, mitigating and managing the ML/TF risks reasonably faced by Crown Melbourne and Crown Perth with respect to these designated services.

a. At no time did the Standard Part A Programs include appropriate risk-based controls to monitor the provision of designated services in HKD, including with respect to designated services provided through international programs or junkets.

b. At no time did the transaction monitoring program in the Standard Part A Programs have regard to the fact that some customers received designated services in HKD for the purposes of determining whether the customer's transactional activity was unusual.

Particulars

For example, there were no processes in place to identify international program or junket customers provided with credit in HKD (item 6, table 1), gaming in HKD (table 3), but repaying credit in AUD (item 7, table 1) or receiving winnings in AUD (items 4 and 9, table 3).

Sections 84(2)(a) and 84(2)(c) of the Act.

Designated services provided in cash

448. From 1 March 2016 to 1 November 2020, the Standard Part A Programs did not include appropriate risk-based systems and controls that were capable by design of identifying, mitigating and managing the ML/TF risks reasonably faced by Crown Melbourne and Crown Perth with respect to designated services designated services involving cash for the reasons pleaded at paragraphs 449 to 455 below.

449. Crown Melbourne and Crown Perth are cash intensive businesses that are vulnerable to the ML/TF risks and typologies pleaded at paragraph 17 and 24.

450. Controls on large cash deposits and payouts at the Crown Melbourne and Crown Perth Cage were not adequate from 1 March 2016 to 1 November 2020:

a. There was no mandatory requirement to obtain information or verification of source of funds for large cash deposits.

b. It was not until December 2020 that Crown Melbourne and Crown Perth issued a policy requiring source of funds information for cash transactions greater than $250,000. If a customer failed to provide appropriate source of funds information, the policy required the transaction to be rejected. In February 2021, the policy was amended to apply to cash transactions over $200,000. In May 2021, the policy was amended again to apply to cash transactions over $150,000.

c. Prior to December 2020, approval levels for large cash transactions at the Cage were inadequate.

d. It was not until November 2020 that cash deposits over $250,000 (in aggregate across a calendar day or in a single transaction) were no longer permitted at the Cage.

e. Prior to November 2020, there were no limits with respect to cash payouts at the Cage, subject to the matters pleaded at f.

f. From 23 November 2018 until 11 November 2020, a $300,000 cap on cash transactions in any 24 hour period was introduced for junket operators, junket representatives and key players. Apart from this cap, the Standard Part A Programs did not include any other appropriate caps or limits on large cash transactions.

451. From 1 March 2016 to 1 November 2020, there were inadequate controls or limits on the deposit and withdrawal of cash relating to DAB, safekeeping and Card Play Extra accounts:

a. It was not until November 2020 that cash deposits over $250,000 (in aggregate across a calendar day or in a single transaction) were no longer permitted with respect to DAB accounts and safekeeping accounts.

b. There were no limits on cash withdrawals from a DAB account.

452. Prior to 1 November 2020, there were no controls to identify or limit cash deposits into Crown Patron accounts, including by third parties.

Particulars

See the particulars at paragraph 219.

453. At all times, controls on cash in private gaming rooms were inadequate, in spite of Crown Melbourne's and Crown Perth's awareness of repeated suspicious activity involving very large amounts of cash.

Particulars

See paragraphs 488 and 532.

454. At all times, controls relating to the carrying of large cash on Crown's private jets were inadequate.

Particulars

See paragraphs 491 and 533.

By no later than June 2018, the Chief Legal Officer of Crown Resorts, who was also the AMLCO for both Crown Melbourne and Crown Perth, was advised by the Group General Manager AML (Crown Melbourne) that the transfer of cash by third parties on Crown's private jet gave rise to potential ML/TF concerns. The Group General Manager AML explained that the potential issue related to source of funds and queried why the funds were not deposited in an account in the departure country. The Group General Manager raised concerns about the carrying of $800,000 cash on the private jet to repay a debt owed to Crown Melbourne.

455. At all times, there were few controls in place for mitigating and managing the ML/TF risks of cash transactions under $10,000:

a. Records were not kept in SYCO of transactions of table 3 designated services under $10,000, unless the customer elected to play carded (that is, against a Crown Rewards membership).

b. In the absence of records, Crown Melbourne and Crown Perth did not have adequate visibility over designated services involving cash under $10,000 and were unable to apply consistent AML/CTF controls.

Particulars

See paragraph 616.

Preventative controls on third party transactions

456. From 1 March 2016 to 1 November 2020, the Standard Part A Programs did not include appropriate risk-based systems and controls that were capable by design of identifying, mitigating and managing the ML/TF risks reasonably faced by Crown Melbourne and Crown Perth with respect to designated services involving third party transactions for the reasons pleaded at paragraphs 457 to 463.

457. From 1 March 2016 to 1 November 2020, Crown Melbourne and Crown Perth facilitated designated services to customers that could involve:

a. the customer using a third party to obtain designated services on their behalf;

b. a third party depositing money into a customer's DAB account or safekeeping account; or

c. a customer transferring money from their DAB account or safekeeping account to a third party.

(**third party transactions**).

Particulars

See paragraph 24.

458. From 1 March 2016 to 1 November 2020, the Standard Part A Programs did not include appropriate preventative controls on third party transactions.

Particulars

See the particulars at paragraph 219.

459. Crown Melbourne and Crown Perth had no appropriate risk-based controls in place to:

a. verify the identity of third parties;

b. understand the source of funds relating to third party transactions; or

c. understand the nature of the relationship between the customer and the third party.

Particulars

Rules 8.1.5, 15.2 and 15.3; and paragraphs (l) and (m) of the definition of KYC information in rule 1.2.1 of the Rules.

460. Crown Melbourne and Crown Perth had no appropriate risk-based processes in place to identify, mitigate and manage the ML/TF risks of third parties with respect to the repayment of loans or the redemption of credit.

Particulars

See paragraph 394.

461. The absence of controls on third party transactions limited Crown Melbourne's and Crown Perth's ability to know their customers and to determine the legitimacy of their transactions.

462. The absence of controls on third party transactions created an avenue for money laundering through smurfing or cuckoo smurfing.

463. From 1 March 2016 to 1 November 2020, Crown Melbourne and Crown Perth processed a significant number of third party transactions through Crown Patron accounts.

Particulars

An external consultant identified the scale of third party deposits on Crown Patron accounts for the period 2014 to 2020.

This review identified 2,551 incoming deposits to Crown Patron accounts from third parties who were individuals. These deposits related to 626 customers and totalled $149,182,411.

Of these 626 customers, 24 customers had five or more unique third party agents (who were individuals) making these deposits, amounting to 541 transactions totalling $15,261,281.

267 incoming deposits to Crown Patron accounts from third parties who were corporates. These deposits related to 127 customers and totalled $68,152,069.

The Southbank accounts were the most prominently used accounts for the deposits made by third party agents. From 2014 to 2021, a total of $63,521,892 was deposited into the Southbank accounts by (individual) third parties on behalf of customers and $45,867,456 was deposited into these accounts by corporate third party agents.

236 of these deposits were made into Crown Patron accounts on behalf of customers who, as identified by the consultant, had adverse media or who had deposits from a third-party individual who has adverse media. These deposits had a total value of $40,222,287 and were made on behalf of 21 customers.

Designated services provided through junket channels

What is a junket?

464. A junket is an arrangement between a casino and a **junket operator** to facilitate a period of gambling by one or more high wealth players (**junket players**) at the casino.

465. Junket operators were at times represented by **junket representatives**.

466. The relationship between Crown Melbourne or Crown Perth and a junket operator was governed by an overarching 'non-exclusive gaming promotion agreement' (**NONEGPRA**).

467. For each junket program, Crown Melbourne or Crown Perth and the junket operator (or authorised junket representative) entered into a Junket Program Agreement (**JPA**).

468. The JPA incorporated the terms and conditions of the NONEGPRA, but the JPA was the agreement that governed a particular junket program.

469. On and from 1 March 2016, Crown Melbourne and Crown Perth facilitated thousands of junket programs.

470. In return for bringing the players to the casino, Crown Melbourne and Crown Perth paid junket operators rebates or commissions.

a. JPAs set out the rebates or commissions available under each junket program.

b. Rebates were calculated based on the junket's gross win/loss, recorded at the time of settlement by Crown Melbourne or Crown Perth.

c. Junkets would agree to bear a percentage of the gross win by Crown (or loss by Crown) of each junket program play by receiving from Crown (or paying Crown) a rebate.

d. A rebate effectively operated as a 'hedge' to reduce the variability of wins/losses by the junket and Crown Melbourne or Crown Perth.

e. Commissions were calculated based on the total turnover of the junket program rather than the gross win/loss at settlement.

f. A commission would be payable by Crown Melbourne or Crown Perth and calculated in accordance with a pre-determined commission rate (a percentage value) and multiplied by the total turnover recorded at the time of settlement.

g. The commission rate would vary depending on whether the front money was cash or amounts drawn from a cheque cashing or credit facility.

   i. The commission rate would be higher in the case of cash.

   ii. If the payment on the cheque cashing or credit facility was received in full within 20 business days from the draw down date, the commission rate would be adjusted to equal the rate applicable to cash front money.

h. The calculations for commissions or rebates would be recorded at the end of the junket program on a junket settlement sheet.

i. Where the front money was drawn down from a cheque cashing or credit facility, the settlement proceeds payable to the junket operator were first applied to the relevant facility. This was also recorded on the junket settlement sheet.

471. A junket financier underwrote credit lines for the junket operators.

Crown Melbourne's and Crown Perth's junket business

472. From 1 March 2016 Crown Melbourne and Crown Perth entered into arrangements with junket operators.

a. On and from 1 March 2016, Crown Melbourne and Crown Perth had relationships with larger 'platform junkets', including the Suncity, Neptune (Neptune Group and Neptune Guangdong Group), Chinatown, Song, Meg-Star, Tak Chun, Jimei, and Oriental Group junkets.

b. Crown Melbourne and Crown Perth also had relationships with smaller junkets.

c. Prior to and from 1 March 2016, Crown Melbourne and Crown Perth sought to attract business from international VIP customers to Australia.

d. Often, international VIPs would seek credit from Crown Melbourne and Crown Perth to fund the purchase of gaming chips.

e. The inherent commercial risk to Crown Melbourne and Crown Perth of non-repayment of gambling debts was amplified for international VIPs who came from jurisdictions in which the enforcement of a gambling debt was practically difficult.

f. Given this, Crown Melbourne and Crown Perth would often decline to offer credit to prospective but unknown international VIPs (being those customers without a reliable debt repayment history with Crown or another casino, or new customers), as Crown Melbourne or Crown Perth could not be satisfied as to their creditworthiness.

g. In these circumstances, Crown Melbourne and Crown Perth would seek to direct these customers to participate in gambling through platform junkets.

h. **Platform junkets** generally referred to larger, more credit-worthy junkets and collections of debts from these junkets were considered by Crown Melbourne and Crown Perth to carry lower credit risk than direct collections from International VIP customers: also see paragraph 470g.

i. Some junket operators were represented by multiple junket representatives.

j. Some junkets had only one key player.

k. In August 2020, the Crown Resorts Board resolved that the Crown Group would cease dealing with junkets on a temporary basis. In November 2020, the Crown Resorts Board determined this ban would be permanent.

l. Following Crown Resorts' resolution, Crown Melbourne and Crown Perth announced they would cease dealing with junkets from August 2020; however, the last junket program play (across Crown Melbourne and Crown Perth) was in March 2020 due to COVID border closures.

m. Crown Melbourne and Crown Perth have held money in DAB accounts for or on behalf of junket operators and representatives on and from August 2020.

Designated services provided through junket channels

473. Crown Melbourne and Crown Perth provided items 6, 7, 31 and 32 table 1, s6 designated services to customers through junket channels in Australian dollars and foreign currencies.

Particulars

Customers who received designated services through junket channels included junket operators, junket representatives, junket financiers and junket players.

See paragraphs 281 to 423.

474. Crown Melbourne and Crown Perth provided table 3 designated services to customers through junket channels in both Australian dollars and HKD.

Particulars

Customers who received designated services through junket channels included junket operators, junket representatives and junket players.

Junket revenue

475. From 1 March 2016 until at least 2019, revenue from designated services provided through junkets channels represented a material source of Crown Melbourne's total revenue.

Particulars

Between July 2015 and June 2020, Crown Melbourne made over $1 billion in junket revenue.

In the 2016, 2017, 2018 and 2019 financial years, junket-generated revenue for Crown Melbourne was approximately $445 million, $200 million, $430 million and $310 million respectively.

In the 2020 financial year, in which revenue was reduced due to COVID-19-related travel restrictions and lockdowns, Crown Melbourne's junket revenue stood at just over $170 million.

In the period 2015 to 2020, Crown Melbourne's reported turnover from VIP program play was $220.8 billion. A substantial proportion of that amount comprised turnover from Asian customers.

The sum of money wagered during junkets over the period 2015 to 2020 was significant. From July 2014 to November 2018, the turnover

of junkets associated with the Suncity junket alone was more than $20 billion.

476. From 1 March 2016 until at least 2019, revenue from designated services provided through junket channels represented a material source of Crown Perth's total revenue.

Particulars

Crown Perth's revenue from junket operations from 1 March 2016 was in excess of $320 million.

The ML/TF risks of junkets

477. The provision of designated services by Crown Melbourne and Crown Perth through junket channels involved higher ML/TF risks pleaded as follows:

a. Junket operators and representatives facilitated the provision of both gaming and financial services to junket players, often in high values.

b. Junkets programs further involved the movement of large amounts of money across borders and through multiple bank accounts, including by third parties.

c. Junket players generally relied on the junket operators to make their funds available at the casinos, including through credit facilities.

d. Junket operators may provide cash to players, in circumstances where the source of funds and the purpose for which the cash is used is unknown.

e. There was a lack of transparency and level of anonymity created by the pooling of all players' funds and transactions under the name of the junket operator.

f. The financial arrangements between the junket operators and junket players were not disclosed to Crown Melbourne or Crown Perth.

g. There are long and complex value chains associated with flows of junket-related funds (involving both gaming and financial services) that makes it difficult for a single reporting entity to understand the purpose of transactions or the beneficial ownership of funds/ultimate beneficiary of value moved.

h. The features of junkets pleaded at c. to g. created layers of obscurity around the identities of persons conducting transactions through junket programs and the source and ownership of funds of customers.

i. On a per-transaction and per-customer basis, the junket tour operations sector is also significantly exposed to the risks associated with high-value cash activity.

j. Junket operators used formal or informal systems to remit money.

k. Junkets programs are vulnerable to cuckoo smurfing and structuring.

l. Money deposited with a junket account and then withdrawn with minimal gaming activity can give the funds the appearance of legitimacy.

m. The use of offsetting arrangements (as explained in paragraph 24) used by junket tour operators to facilitate junket-related funds:

   i. is highly likely to be exploited by criminal entities;

   ii. can circumvent international funds transfer reporting requirements; and

iii. can facilitate the laundering of domestically-generated proceeds of crime.

n. Junket accounts at casinos are highly vulnerable to the storage and movement of potentially illicit funds. The 'parking' of illicit money puts distance between the act or acts that generated the illicit funds and the ultimate recipients of those funds, making it harder to trace the flow of money.

o. Inherent to the junket tour operations sector is exposure to some higher ML/TF risk jurisdictions.

p. There is a particular vulnerability associated with jurisdictions with currency flight and gambling restrictions in place as these measures create demand for covert money remittances which can be exploited by criminal groups.

q. Having a customer base composed of predominantly foreign residents can increase the junket sector's attractiveness and exposure to transnational serious and organised crime, simply due to its geographical reach.

r. In addition, such a customer base can mean that the source and destination of funds, and information about customers' criminal and financial activity, are difficult to identify as they are located in foreign jurisdictions.

s. As the level of gaming transactions during junkets is relatively high, there is also a higher risk that junkets will be exploited for money laundering.

Particulars

FATF/ APG Casino Typologies Report.

AUSTRAC Junket Assessment.

FATF RBA Guidance.

ML/TF risk assessments and controls

478. Crown Melbourne and Crown Perth did not carry out an appropriate ML/TF risk assessment of the higher ML/TF risks of providing designated services through the junket channel in the period from 1 March 2016 to 1 November 2020.

479. Consequently, from 1 March 2016 to 1 November 2020, the Standard Part A Programs did not include appropriate risk-based controls to identify, mitigate and manage the ML/TF risks of designated services provided through the junket channel for the reasons pleaded at paragraphs 481 to 494.

480. In spite of the known higher ML/TF risks as pleaded at paragraph 477, the controls in the Standard Part A Programs that applied to the provision of designated services through junkets were generally no different to the controls applied to other customers.

Customer risk

481. At no time did the Standard Part A Programs include appropriate systems and controls to identify, mitigate and manage the ML/TF risks of customers receiving designated services through junket channels:

a. The customers receiving designated services through junket channels included junket operators, junket representatives and junket players.

b. Customers receiving designated services through junket programs were considered low risk by default.

Particulars

Clause 13 of the Standard Part A Programs.

Customers receiving designated services through junket programs were not low risk, including for the reasons pleaded at paragraph 477.

c. At no time did Crown Melbourne or Crown Perth assess the jurisdictional risks associated with customers receiving designated services provided through the junket channel.

d. The Standard Part A Programs did not include appropriate risk-based controls to obtain and analyse source of wealth and funds information with respect to junket operators, representatives and players.

e. The Standard Part A Programs did not include appropriate risk-based controls to collect and verify appropriate KYC information with respect to junket operators and other customers receiving designated services through junket channels, such as the beneficial ownership of funds or the beneficiaries of transactions.

Particulars

Rules 8.1.5, 15.2 and 15.3 and paragraphs (l) and (m) of the definition of *KYC information* in rule 1.2.1 of the Rules.

f. Crown Melbourne and Crown Perth provided designated services to junket players in circumstances where it did not have a direct relationship with the customer, but relied upon the junket operator as an intermediary or agent. As a consequence, Crown Melbourne and Crown Perth did not always know who it was providing designated services to via junket channels.

g. At no time did Crown Melbourne or Crown Perth appropriately identify, mitigate and manage the ML/TF risks of providing designated services to junket players through junket operators and representatives as agents.

Particulars

Crown Melbourne and Crown Perth permitted junket operators to pay out winnings to junket players, without first assessing this risk.

Crown Melbourne and Crown Perth permitted junket operators to exchange cash for chips or vice versa for junket players, without first assessing this risk.

Complex transaction chains

482. Crown Melbourne and Crown Perth provided a range of table 1 and table 3, s6 designated services to customers through junket channels, involving complex transaction chains, but at no time identified, mitigated or managed the associated ML/TF risks.

Particulars

Rule 8.1.3 of the Rules.

Records of play on junket programs

483. Crown Melbourne and Crown Perth were reliant upon records maintained by the junket operator or representative as to the table 3, s6 designated services Crown Melbourne and Crown Perth provided to junket players, including with respect to the junket players' turnover, winnings and losses.

Particulars

The gaming activity of individual players on junkets was recorded on SYCO via junket operator records and key player ratings (i.e. records of the type and amount of the player's play, betting and wins/losses).

To facilitate this, a 'Junket Card' was issued to each player named on the JPA, which listed the player's name and the gaming system number of the junket operator. The purpose of the Junket Card was to ensure that play by junket players was attributed to the junket operator for the purposes of commissions.

At the end of each junket program, all gaming activity of the junket as a whole was recorded onto a settlement sheet which captured turnover, wins and losses, expenses deducted, expenses reimbursed and commissions or rebates.

To the extent that Crown Melbourne and Crown Perth recorded the provision of table 3 designated services to individual junket players, it was reliant upon junket operator records.

Also see the limitations of recording transactional data on ATOM at paragraph 615.

484. The Standard Part A Programs did not require Crown Melbourne or Crown Perth to make and keep appropriate records of the designated services provided to each junket player under a junket program.

485. Crown Melbourne and Crown Perth did not have appropriate systems and controls in place to ensure that junket operator records reliably attributed play to key players.

486. In the absence of appropriate records of the designated services Crown Melbourne and Crown Perth provided through junket program channels, Crown Melbourne and Crown Perth were unable to adopt and maintain appropriate risk-based AML/CTF controls.

Credit facilities and CCFs

487. At no time did the Standard Part A Programs appropriately identify, mitigate and manage the ML/TF risks of providing credit facilities and CCFs to junket operators or representatives (item 6 and 7, table 1, s6):

a. A credit facility or CCF was opened in the name of the junket operator, and the junket operator could delegate to a junket representative authority to operate the facility either up to the full amount of the facility or some lesser specified amount.

b. Crown Melbourne and Crown Perth did not provide junket players with direct access to the approved junket credit facilities. However, following each drawdown of a credit facility or CCF by the junket operator or junket representative, the CPVs, gaming chips or cash equivalents issued by Crown — to be used for the relevant junket program —

would be provided at the junket operator's or representative's discretion to the junket players.

c. At all times, Crown Melbourne and Crown Perth did not have any processes in place to identify how, for example, the gaming chips issued by Crown, based on the approved junket credit, were subsequently distributed among the junket players by the junket operator or representative.

d. Crown Melbourne and Crown Perth had no visibility as to how the junket operators funded junket players' front money or as to how junket players were paid their winnings.

e. Where a junket operator was involved in funding a junket player's front money, the junket operator also paid out winnings to the junket player.

f. Crown Melbourne or Crown Perth did not appropriately identify and assess the ML/TF risks associated with junket operators redeeming or repaying credit, or the channels through which the credit was repaid, including through the overseas deposit services.

g. When a customer applied for credit, Crown Melbourne and Crown Perth conducted a risk assessment focussed on credit risk not ML/TF risk.

Large cash transactions

488. From 20 April 2018, Crown Melbourne introduced a ban on cash transactions in the private Suncity room, with the exception of petty cash transactions of up to $100,000.

Particulars

Junket tour operators had arrangements with junket players whereby cash could be advanced to the junket players (or their travel companions) for use while on their visit to Australia, such as for shopping, dining or admission tickets at tourist attractions. Money advanced on this basis would typically have been accounted for when the junket settled their winnings or losses accrued during the junket program with the junket player. However, based on the recollection of employees, Crown Melbourne understood that sometimes the petty cash was paid to a player in exchange for chips held by the player - in effect cashing in the chips.

Petty cash was kept in the top drawer of the Suncity cash administration desk.

For a description of the Suncity room, see paragraph 526.

For a description of the Suncity cash administration desk, see paragraph 529.

489. From November-December 2018 until 11 November 2020, a $300,000 cap on cash transactions in any 24 hour period was introduced at Crown Melbourne and Crown Perth for junket operators, junket representatives and key players.

Particulars

From April 2018 Crown Melbourne required all cash transactions in the Suncity room to be conducted through the Crown Melbourne Cage, not the Suncity cash administration desk.

It is not clear how this control was consistently enforced - see the particulars at paragraph 488.

From April 2018, Crown Melbourne also introduced additional identification controls for entry into the Suncity room.

From December 2018, Crown Melbourne introduced a further requirement that any bag taken into the Suncity room be transparent so that video surveillance could monitor the contents of bags upon person entering and exiting the rooms.

It is not clear how this requirement was enforced.

In March 2019 controls were enhanced to maintain higher video surveillance and access control to the Suncity room.

490. The controls pleaded at paragraph 488 and 489 did not appropriately mitigate and manage the ML/TF risks of large cash transactions in private gaming rooms through junket channels.

491. The Standard Part A Programs did not include any other controls to appropriately identify, mitigate and manage the ML/TF risks of large cash transactions through junket channels:

a. Controls on large cash transactions and on large amounts of cash being brought into and out of private gaming rooms were inadequate.

Particulars

See paragraphs 493 and 532.

b. From December 2018/early 2019, a potential risk was added to the Risk Registers, relating to 'risks not associated with provision of designated services'. The risk was described as 'witnessing large cash transactions by junket operators, junket representatives or junket staff members (not Crown Melbourne/Crown Perth employees) with unknown third parties'. The specific controls responsive to this risk were described as 'surveillance and security staff trained to identify and report suspicious behaviour'.

Particulars

Surveillance and staff observation were inadequate controls to identify, mitigate and manage the ML/TF risks associated with large cash transactions. The reporting of SMRs to the AUSTRAC CEO did not discharge Crown Melbourne's and Crown Perth's responsibility to identify, mitigate and manage the ML/TF risks of their business.

It was not clear how the $300,000 cap on cash transactions for junket operators, junket representatives and key players was implemented or enforced with respect to the ML/TF risks of cash transactions that Crown Melbourne and Crown Perth classified as being associated with the provision of designated services.

c. There were no controls with respect to the carrying of large amounts of cash on Crown's private jets, including by third parties on behalf of Crown customers.

Remittance services

492. At no time did Crown Melbourne or Crown Perth identify, mitigate and manage the ML/TF risks of providing remittance services (items 31 and 32, table 1, s6) through junket channels:

a. Crown Melbourne and Crown Perth permitted junket operators and junket representatives to transfer money between:

i. DAB accounts in their names; and

ii. DAB accounts in the names of junket players, other junket operators and representatives, and other third parties.

b. Crown Melbourne and Crown Perth also permitted:

i. third party telegraphic transfers into DAB accounts held by junket operators and representatives, including from junket players and from other persons who were not key players under the relevant junket program (item 13, table 3, s6 and items 31 and 32, table 1, s6 designated services); and

ii. third party telegraphic transfers from DAB accounts held by junket operators and representatives, including to junket players and other persons who were not key players under the relevant junket program (item 13, table 3, s6 and items 31 and 32, table 1, s6 designated services).

c. At no time did Crown Melbourne or Crown Perth identify and assess the ML/TF risks of transactions on DAB accounts held by junket operators or representatives.

d. The Standard Part A Programs did not include appropriate operational controls to limit or mitigate and manage the ML/TF risks of third party transfers and/or deposits at any time prior to November 2020.

Particulars

See the particulars at paragraph 219.

e. In reliance upon records maintained by junket operators or representatives, Crown Melbourne and Crown Perth facilitated the payment of a junket player's winnings by transferring funds from a junket operator's DAB account (item 13, table 3, s6) by telegraphic transfer to either the junket player or other third party (items 31 and 32, table 1, s6).

f. At no time did Crown Melbourne or Crown Perth assess the ML/TF risks of providing item 31 and 32 table 1, s6 designated services to junket operators, representatives or players through non-transparent channels including the Southbank and Riverbank accounts and the Suncity account.

Particulars

An external auditor identified 136 beneficiaries who had received telegraphic transfers from junket operators, and who were not recorded by Crown Melbourne or Crown Perth as players on the junket, or were not otherwise known customers of Crown Melbourne or Crown Perth. The transactions to these beneficiaries amounted to a total of AUD$134,721,037 and HKD$38,637,044.

As the beneficiaries of these transfers could not be identified, the nature and purpose of these transactions - and whether they had a legitimate economic purpose - was unclear.

Private gaming rooms and cash administration desks

493. At no time did Crown Melbourne and Crown Perth identify, mitigate and manage the ML/TF risks of providing designated services through the junket channel in private gaming rooms, including but not limited to the risks of cash in private gaming rooms.

a. At no time were specific ML/TF risk assessments conducted with respect to private gaming rooms.

b. At no time did Crown Melbourne identify and assess the ML/TF risks of permitting junket operators and representatives to operate cash administration desks within private gaming rooms.

Particulars

See paragraphs 529 (Suncity cash administration desk) and 561 (Meg-Star cash administration desk).

c. At no time did Crown Perth identify and assess the ML/TF risks of permitting junket operator Person 36 to operate an administration desk within a private gaming room that was used to facilitate and record the number and value of the gaming chips that were distributed to and received back from each junket player.

d. Controls to address the ML/TF risks of providing certain designated services in private gaming rooms occupied by junkets were generally limited to surveillance and identifying junket players and their guests prior to entry into the room.

e. From mid-2018, some additional controls were developed for the Suncity room, including the following. However, they did not appropriately mitigate and manage the full extent of the ML/TF risks relating to large cash transactions and large cash being brought into and out of in these rooms.

i. The removal of the note counting machine from the Suncity cash administration desk, implemented from 20 April 2018;

ii. A $100,000 total petty cash limit at the Suncity cash administration desk, implemented from 20 April 2018;

iii. The requirement that all gaming cash transactions must occur at the Crown Melbourne Cage rather than the Suncity cash administration desk implemented from 20 April 2018; and

iv. The requirement to use transparent bags in the Suncity room so that security and surveillance could monitor what was being taken into the Suncity room implemented from late 2018.

Particulars

See paragraph 521.

Junket due diligence

494. The due diligence conducted with respect to junket operators and representatives did not appropriately identify, mitigate and manage the ML/TF risks with respect to designated services provided through the junket channel including for the following reasons:

a. Crown Melbourne and Crown Perth conducted due diligence only on junket operators and not on junket representatives, unless a representative was applying for credit.

b. Crown Melbourne and Crown Perth did not conduct due diligence on corporate junket operators, but only on the individual who applied for approval to become an operator.

c. Due diligence on junket operators, including at the time of annual review, was carried out by VIP International; was focussed on credit risk; and was not guided by appropriate criteria relevant to ML/TF risk.

d. Appropriate records of due diligence on junket operators were not kept.

e. ECDD (including on junket players) was not consistently recorded in Crown's customer management system, SYCO, or on CURA.

f. The Standard Part A Programs did not include appropriate systems and controls for due diligence on junket financiers.

g. Crown Melbourne and Perth did not necessarily know the identity of persons who were financing junkets and did not take appropriate steps to understand the junkets' source of funds.

Oversight frameworks for international VIP customers and junkets

495. The Standard Part A Programs did not include, or incorporate an appropriate framework for roles, accountabilities and reporting lines with respect to the management of ML/TF risks or ML/TF risk appetite for international VIP and junket customers of Crown Melbourne and Crown Perth for the reasons pleaded at paragraph 496 to 520 below.

VIP International

496. Until 14 January 2021, the VIP International business was a separate business unit within Crown Resorts which reported directly to the CEO of Australian Resorts.

497. VIP International was responsible for managing the business of international VIP customers visiting Crown Melbourne and Crown Perth. This included participants in junket programs and premium player programs.

498. VIP International was a group function based in Melbourne.

499. Within Crown Perth, VIP International was referred to as the International Commission Business (**ICB**).

500. The principal responsibility of the Crown Perth's ICB team was to provide on-the-ground hosting of junkets.

501. Crown Melbourne and Crown Perth relied on VIP International to make decisions relating to credit approvals for international customers, junket operator due diligence, junket management and strategic planning.

Particulars

See paragraphs 498 to 500.

502. Until October 2016, the **VIP Working Group** provided guidance and advice to VIP International in relation to international and VIP customers, including strategies for particular VIP markets and related risk appetite.

503. The VIP Working Group members included management within Crown Resorts and Consolidated Press Holdings Pty Ltd (**CPH**).

504. Between late 2016 and mid 2017 a series of meetings was convened, referred to as the **VIP Operations meetings**.

505. These meetings were attended by senior management from various Crown entities including Crown Melbourne and Crown Resorts.

506. The authorisation of existing junket operators was reviewed at the VIP Operations meetings.

507. The attendees of the VIP Operations meetings were briefed with customer profiles prepared by the Credit Control team, within VIP International.

508. At the VIP Operations meetings, decisions were made on whether Crown Melbourne and Crown Perth should continue dealing with junket operators who were the subjects of review.

509. The Standard Part A Programs did not include or incorporate a framework for Crown Melbourne or Crown Perth to determine whether the decisions made by VIP International, relating to:

a. Crown Melbourne or Crown Perth customers; or

b. designated services provided by Crown Melbourne or Crown Perth through junket channels

were within the ML/TF risk appetite of Crown Melbourne or Crown Perth.

Particulars

Crown Resorts had oversight of VIP International and determined the risks to be accepted by Crown Melbourne and Crown Perth in relation to junket operators, representatives and players.

There were no formal reporting lines from Crown Melbourne or Crown Perth to the VIP Working Group, and it operated outside a formal reporting structure.

Decisions made at the VIP Operations meetings were focussed on the credit risk, not ML/TF risks, of junket operators.

Approval of credit facilities and CCFs for international customers

510. The senior management approving credit facilities and CCFs for international and VIP customers included members of Australian Resorts, Crown Resorts and VIP International.

511. Applications by international customers for credit facilities or CCFs were reviewed and approved jointly for Crown Melbourne and Crown Perth:

a. The application process for credit facilities was uniform across Crown Perth and Crown Melbourne.

b. CCF limits for international customers were approved for both Crown Melbourne and Crown Perth and the global limit could be used across both properties.

c. The Credit Control team (a team within Crown Resorts and based in Melbourne) received applications made by customers to Crown Perth.

d. The Credit Control team created a central credit profile for customers, conducted the requisite credit checks and then sent the customer's credit profile and report to Crown Perth with a recommended facility limit.

512. There was no framework in place in the Standard Part A Programs for Crown Melbourne or Crown Perth to determine whether decisions with respect to:

a. the approval of credit facilities or CCFs for international customers; and

b. the credit limit that would apply to credit facilities or CCFs for international customers

were within the ML/TF risk appetite of Crown Melbourne or Crown Perth.

The Suncity Deposit service channel

513. In May 2017 an account was opened with Suncity in Macau in the personal name of a Crown Resorts employee to facilitate an overseas deposit service for Crown Melbourne and Crown Perth customers, as described in full at paragraph 423.

514. The Suncity Deposit Service had the higher ML/TF risks described at paragraph 423.

515. There was no framework in place in the Standard Part A Programs for Crown Melbourne or Crown Perth to determine whether the decision made by VIP Finance to establish the Suncity Deposit Service was within their ML/TF risk appetite.

Hotel Card Transaction channel

516. In 2012, senior Crown Resorts executives instituted an arrangement for international VIP customers to use a credit or debit card at the Crown Towers Hotel to authorise a transfer of funds to be made available to the same customers at the Crown Melbourne Casino.

517. This arrangement operated from 2012 to October 2016.

518. The arrangement involved Crown Melbourne providing item 32, table 1, s6 designated services from 1 March 2016 to October 2016.

Particulars

See paragraph 416.

519. This channel involved the acceptance by Crown Melbourne of higher ML/TF risks, which were never the subject of an ML/TF risk assessment.

520. There was no framework in place in the Standard Part A Programs for Crown Melbourne to determine whether the decisions made by Crown Resorts to continue operating the HCT channel from 1 March 2016 to October 2016 was within their ML/TF risk appetite.

The Suncity junket

521. At all times until November 2020, Crown Melbourne and Crown Perth had a NONEGPRA with by Customer 1, who operated a junket branded as the 'Suncity' junket (the **Suncity junket**).

522. From 1 March 2016 to November 2020:

a. Crown Melbourne facilitated approximately 190 junket programs with the Suncity junket, in respect of which:

   i. total turnover exceeded $20 billion;

   ii. total customer losses (Crown wins) were just over $360 million; and

   iii. Customer 1 was paid commissions exceeding $210 million.

b. Crown Perth facilitated over 80 junket programs with the Suncity junket, in respect of which:

   i. total turnover exceeded $2 billion;

   ii. total customer losses (Crown wins) were just under $72 million; and

   iii. Customer 1 was paid commissions exceeding $25 million.

523. At all times, Crown Melbourne and Crown Perth understood that Customer 1 was the ultimate beneficial owner for the Suncity junket.

524. At all times until January 2021, Crown Melbourne and Crown Perth provided table 1 and table 3, s6 designated services to customers through the Suncity junket.

525. In November 2021:

a. Customer 1 was arrested by a foreign country in connection with allegations relating to an illegal gambling syndicate and money laundering; and

b. Authorities in a second foreign country issued an arrest warrant for Customer 1, in connection with alleged illicit cross-border and online gambling operations.

The private Suncity gaming room at Crown Melbourne

526. At all times, Crown Melbourne made private gaming rooms available to the Suncity junket (the **Suncity room**).

a. From January 2014 until 2 July 2018, Suncity had exclusive use of a dedicated gaming room at Crown Melbourne, located in Pit 86, a salon located adjacent to the Teak Room.

b. From 2 July 2018, Suncity room was relocated to Pit 38, which was a salon located in the Mahogany room.

c. On 12 March 2019, the Suncity room was moved back to Pit 86.

d. Suncity ceased to use Pit 86 on an exclusive basis in August 2019, after which they did not have a dedicated private room at Crown Melbourne.

e. From August 2019 the Suncity junket continued to use Pit 86 on a non-exclusive basis, until March 2020 when the casino was closed due to COVID-19.

f. Customers of Crown Melbourne and guests were permitted entry to the Suncity room.

527. At all times, Crown Melbourne provided table 3, s6 designated services to customers in the Suncity room.

The private Suncity gaming rooms at Crown Perth

528. At all times, Crown Perth made private gaming rooms available to the Suncity junket on a non-exclusive basis.

The Suncity cash administration desk at Crown Melbourne

529. From February 2014 to March 2020 (when the casino was closed due to the COVID-19 pandemic), Crown Melbourne allowed the Suncity junket to operate a cash or administration desk in the private Suncity room (the **Suncity cash administration desk**).

a. Until April 2018, Suncity staff members would dispense commission chips in exchange for cash to junket players.

b. In addition, until April 2018 at the Suncity cash administration desk junket players could exchange chips for cash, and could deposit cash with the junket.

c. In March 2018, Crown Melbourne advised Suncity that cash transactions in the Suncity room located at Pit 86 were banned (other than for petty cash transactions up to A$100,000).

d. On 20 April 2018, Crown senior management again spoke with Suncity staff to ensure that they were aware of the changes in relation to cash, and carried out an audit of the Suncity cash administration desk in which approximately $5.6 million in cash was identified and taken to the Crown Cage in the Mahogany Room by Crown Melbourne security. The cash was subsequently deposited into Customer 1's safekeeping account.

530. From February 2014 to March 2020, Crown Melbourne operated a Crown cashier desk in the Suncity room (referred to as a 'cage' or the 'buy-in window'), which was staffed by Crown Melbourne personnel.

531. The Suncity cash administration desk was a channel through which Crown Melbourne provided designated services to customers.

The ML/TF risks posed by the Suncity junket

532. From 1 March 2016, the provision of designated services by Crown Melbourne and Crown Perth through the Suncity junket posed higher ML/TF risks, including for the following reasons:

a. Designated services provided by Crown Melbourne and Crown Perth through the Suncity junket involved the ML/TF risks as pleaded at paragraph 477.

b. The involvement of Customer 1, who Crown Melbourne and Crown Perth understood to be the ultimate beneficial owner of the Suncity junket, in circumstances where at all times on and from 1 March 2016, Crown Melbourne and Crown Perth were aware of allegations that Customer 1:

i. was a former member of organised crime networks;

ii. was associated with individuals linked to organised crime;

iii. was a foreign PEP; and

iv. had allegedly indirectly received funds stolen from a central bank.

Particulars

See Customer 1.

c. Crown Melbourne had limited visibility over activity in the Suncity room.

d. Prior to July 2018, Crown Melbourne had limited visibility as to the persons who were entering the Suncity room.

e. At all times, large cash transactions and transactions involving cash that appeared suspicious were facilitated through the Suncity room at Crown Melbourne, including large volumes of cash in small notes in rubber bands/plastic bags/shoe boxes and counterfeit cash at the Suncity cash administration desk.

i. From 1 March 2016 to December 2018, there were at least 75 suspicious 'incidents' in the Suncity room, known to Crown Melbourne, involving cash in excess of $23 million.

Particulars

See Customer 1.

These incidents involved highly suspicious activity, including large amounts of cash brought into the Suncity room by unknown persons; large amounts of cash being exchanged between junket representatives and unknown persons in the Suncity room; and large amounts of cash being carried in suitcases, envelopes, Crown carry bags, brown paper bags or shoe boxes.

ii. In the six months prior to May 2018, Crown Melbourne gave the AUSTRAC CEO 58 SMRs concerning behaviour in the Suncity room, relating to transactions totalling $16.8 million, yet failed to take appropriate steps to identify, mitigate and manage the ML/TF risks of which it was aware.

Particulars

By no later than June 2018, the Chief Legal Officer of Crown Resorts, who was also the AMLCO for both Crown Melbourne and Crown Perth, was briefed on the suspicious activity in the Suncity room.

iii. In May 2017, Customer 24 was identified in footage of the Suncity room handing out money from a cooler bag full of cash. In May 2018, Customer 24 was arrested in the Suncity room in connection to a money laundering investigation.

Particulars

See Customer 24.

iv. From October 2017, Customer 23 (a key player on the Suncity junket) deposited approximately $760,000 at the Suncity cash administration desk over six transactions using cash that appeared suspicious.

Particulars

See Customer 23.

v. From November 2017, Customer 22 made a number of deposits and withdrawals at the Suncity cash administration desk, using cash that appeared suspicious, despite not being a player on any Suncity junkets.

Particulars

See Customer 22.

vi. From December 2017, on multiple occasions, Customer 25 or a Suncity junket representative acting on Customer 25's behalf deposited cash that appeared suspicious at the Suncity cash administration desk.

Particulars

See Customer 25.

vii. In January 2018, Crown Melbourne received an enquiry from law enforcement in relation to a cash deposit in the Suncity room by a key player, Customer 20, with suspected involvement from Customer 1.

Particulars

See Customer 1 and Customer 20.

viii. In December 2018, two men (including Customer 23) were arrested attempting to deposit at a bank branch $250,000 in cash that had been retrieved from a backpack, which was removed from behind a curtain in the Suncity room.

Particulars

Despite reviewing CCTV footage, Crown was unable to determine when the backpack first arrived in the Suncity room.

Following this incident, Crown Melbourne instituted a requirement that only clear plastic bags could be taken into the Suncity room.

See Customer 1 and Customer 23.

f. Crown Melbourne did not make or keep appropriate records in relation to transactions in the Suncity room.

g. Crown Melbourne did not make or keep any records in relation to transactions, including cash transactions, facilitated through the Suncity cash administration desk.

h. Crown Melbourne had limited or no visibility over transactions through the Suncity cash or administration desk.

i. Between 1 March 2016 and 27 November 2020, Crown Melbourne gave 210 SMRs to the AUSTRAC CEO relating to designated services provided through the Suncity junket.

Particulars

The grounds of suspicion included annual losses by key players on Suncity junkets, telegraphic transfers with third parties and large cash deposits and withdrawals from Customer 1's DAB account.

See Customer 1.

j. At all times, large telegraphic transfers were facilitated into and out of the DAB account held by Customer 1 to operate the Suncity junket, including:

i. to and from key players on the Suncity junket, in respect of whom Crown Melbourne had formed suspicions, including Customer 20;

Particulars

See Customer 20.

ii. to and from third parties unrelated to the junket:

A. From 1 March 2016, Crown Melbourne lodged SMRs in relation to a number of telegraphic transfers from Customer 1 to third parties totalling $7,796,163.

B. From 1 March 2016, Crown Melbourne lodged SMRs in relation to a number of telegraphic transfers from third parties to Customer 1 totalling $14,995,924.40.

Particulars

See Customer 1.

k. At all times, large transfers were made between the DAB account held by Customer 1 to operate the Suncity junket, and DAB accounts at Crown Melbourne and Crown Perth held by key players on Suncity junket programs, other junket operators and third parties.

Particulars

See Customer 1.

l. At all times, the Suncity junket, its representatives, and key players, including Customer 20, Customer 22, Customer 23, Customer 24 and Customer 25, and third parties engaged in transactions indicative of ML/TF typologies and vulnerabilities at Crown Melbourne and Crown Perth.

Particulars

See Customer 1, Customer 20, Customer 22, Customer 23, Customer 24 and Customer 25.

533. In 2016, on four occasions, Crown Melbourne made the Crown private jet available for the use of Customer 1 and the Suncity junket.

Particulars

See Customer 1.

See also paragraphs 454 and 491.

534. Crown Melbourne purported to carry out ML/TF risk assessments on its business relationship with the Suncity junket in around April 2018 and early 2019.

535. At no time did Crown Melbourne carry out an appropriate assessment of the ML/TF risks it reasonably faced with respect to the designated services it provided through the Suncity junket channel.

536. Crown Melbourne did not carry out an ML/TF risk assessment in relation to the Suncity cash administration desk prior to the introduction of this facility at the Crown Melbourne Casino.

537. At no time did Crown Melbourne conduct an appropriate risk assessment of the designated services it provided through the Suncity cash administration desk.

538. At no time did Crown Perth carry out an appropriate assessment of the ML/TF risks it reasonably faced with respect to the designated services it provided through the Suncity junket.

ML/TF controls with respect to the Suncity junket

539. The Standard Part A Programs did not include appropriate risk-based systems and controls to identify, mitigate and manage the ML/TF risks of designated services provided through the Suncity junket.

a. At no time did Crown Melbourne or Crown Perth carry out appropriate due diligence with respect to Customer 1, as operator of the Suncity junket, having regard to the ML/TF risks posed by Customer 1 and the Suncity junket.

Particulars

See Customer 1.

b. Prior to July 2018:

i. there was no requirement in the Part A Programs for persons entering the Suncity room in Melbourne to be identified; and

ii. the Crown Melbourne security officer stationed outside the Suncity room monitored for minors and general security issues only.

c. From July 2018, Crown Melbourne introduced a requirement for customers and guests to be identified upon entry.

i. Upon entry, customers were required to provide appropriate identification and/or the customer's Crown Rewards card or VIP Card.

ii. Guests of existing Crown Rewards customers or VIP customers were required to provide appropriate identification to be registered as a guest.

iii. However, there was no process to verify the identification presented by customers or guests, nor were there adequate processes in place to ensure this requirement was consistently followed.

d. From March 2019, improvements had been made at Pit 86 so that these entry controls could be followed.

i. From March 2019, the salon doors were controlled by a surveillance camera and buzzer, and the doors could only be opened by swiping a Crown ID card, or by a staff member within the gaming salon pushing a button to open the door.

ii. A Crown reception desk was set up outside the salon to control entry to the salon, including through conducting identification checks and registering new customers, and through signing-in guests.

iii. However, there was no process to verify the identification presented by customers or guests.

e. CCTV surveillance outside the Suncity room (and inside the Suncity room from March 2019) was not an adequate AML/CTF control on its own.

f. Crown Melbourne staff were not adequately trained on ML/TF risks and AML/CTF controls.

g. In the absence of appropriate records of the designated services Crown Melbourne provided through the Suncity room and through the Suncity cash administration desk, Crown Melbourne was unable to adopt and maintain appropriate risk-based AML/CTF controls.

Particulars

See paragraphs 483 to 486 and 493.

h. Footage from CCTV and table cameras did not constitute appropriate records of designated services provided in the Suncity room.

i. At no time did the Standard Part A Programs apply appropriate risk-based transaction monitoring in the Suncity room.

j. At no time did Crown Melbourne adopt and maintain appropriate risk-based controls to identify, mitigate and manage the ML/TF risks of cash transactions in the Suncity room.

Particulars

See paragraphs 488 to 491.

540. In November 2020, Crown Melbourne and Crown Perth imposed stop codes on DAB accounts and Safekeeping accounts held by Customer 1.

541. On 22 January 2021, Crown Melbourne issued a WOL with respect to Customer 1.

542. On 29 January 2021, Crown Perth issued a NRL with respect to Customer 1.

543. Crown Melbourne and Crown Perth should have assessed whether an ongoing business relationship with the Suncity junket, including through Customer 1, was consistent with ML/TF risk appetite at a much earlier point than November 2020.

The Song junket

544. The Standard Part A Programs did not include appropriate risk-based systems and controls to identify, mitigate and manage the ML/TF risks of designated services provided by Crown Melbourne and Crown Perth through the Song junket for the reasons pleaded at paragraphs 545 to 554.

545. On and from 1 March 2016, Crown Melbourne and Crown Perth had a NONEGPRA with Customer 2, who was the operator of the Song junket.

Particulars

See Customer 2.

546. Crown Melbourne facilitated 68 junket programs for the Song junket, and Crown Perth facilitated four junket programs for the Song junket, in respect of which:

a. By no later than March 2020, turnover at Crown Melbourne for the Song junket had exceeded approximately $10,561,102,323.

b. By no later than March 2020, turnover at Crown Perth for the Song junket had exceeded $74,123,400.

547. At all times Crown Melbourne and Crown Perth understood that Customer 2 was the ultimate beneficial owner of the Song junket.

548. At all times from March 2016 to January 2021, Crown Melbourne and Crown Perth provided table 1 and table 3, s6 designated services to customers through junket programs operated by Customer 2.

Particulars

See Customer 2.

549. The provision of designated services by Crown Melbourne and Crown Perth through the Song junket posed higher ML/TF risks, including for the following reasons:

a. Designated services provided by Crown Melbourne and Crown Perth through the Song junket involved the ML/TF risks as pleaded at paragraph 477.

b. By late December 2016, Crown Melbourne and Crown Perth became aware of allegations that Customer 2, who was the approved operator and representative of the Song junket for both Crown Melbourne and Crown Perth, had been convicted and sentenced in 2003 for illegal gambling in an overseas country.

c. By late December 2016, Crown Melbourne and Crown Perth became aware that funds from Customer 2's DAB account were the subject of proceeds of crime proceedings in Victoria in 2016 on the basis of suspected money laundering and tax avoidance.

d. Between 18 May 2010 and 16 February 2016, Crown Melbourne gave the AUSTRAC CEO 77 SMRs relating to designated services provided through the Song junket.

Particulars

The grounds of suspicion included funds being transferred between multiple customers, funds being transferred in circumstances where total player transactions were not proportional to the amount being transferred, and telegraphic transfers being made to and from Customer 2's DAB account involving third parties who were unrelated to the Song junket.

See Customer 2.

e. Between 27 April 2016 and 20 March 2020, Crown Melbourne and Crown Perth gave the AUSTRAC CEO 235 SMRs relating to designated services provided through the Song junket.

Particulars

The grounds of suspicion included telegraphic transfers made to and from Customer 2's DAB account involving third parties were unrelated to the Song junket, cash deposits in usual circumstances and transactions involving multiple customers who also played on other junkets.

See Customer 2.

f. Large telegraphic transfers into and out of DAB accounts held by Customer 2 including to and from third parties unrelated to the Song junket.

Particulars

See Customer 2.

g. Large cash transactions involving the Song junket and its representatives.

Particulars

See Customer 2.

h. Transactions indicative of ML/TF typologies and vulnerabilities involving the Song junket and its representatives.

Particulars

See Customer 2.

550. From 1 March 2016, from time to time, Crown Melbourne made a villa in Crown Towers available to representatives of the Song junket.

551. Crown Melbourne does not know whether or not designated services were provided through the villa.

552. Crown Melbourne did not carry out an ML/TF risk assessment in relation to the villa.

553. Persons affiliated with the Song junket were given access to the Crown private jet in 2018 and 2019.

Particulars

See Customer 2.

See paragraphs 454 and 491.

554. Having regard to the matters pleaded at paragraph 477, the Standard Part A Programs did not include appropriate risk-based controls to identify, mitigate and manage the higher ML/TF risks posed by the matters pleaded at paragraphs 549 to 553.

Particulars

See paragraphs 477 to 494.

The Meg-Star junket

555. From 1 March 2016 to 1 November 2020, the Standard Part A Programs did not include appropriate risk-based systems and controls to identify, mitigate and manage the ML/TF risks of designated services provided by Crown Melbourne and Crown Perth through the Meg-Star junket for the reasons pleaded at paragraphs 556 to 563 below.

556. On and from 1 March 2016, Crown Melbourne and Crown Perth had a NONEGPRA with Customer 3, who was the operator of the Meg-Star junket.

Particulars

See Customer 3.

557. Crown Melbourne facilitated 221 junket programs for the Meg-Star junket and Crown Perth facilitated 61 junket programs for the Meg-Star junket, in respect of which:

a. By no later than December 2020, total turnover at Crown Melbourne exceeded $10,000,000,000; and

b. By no later than December 2020, total turnover at Crown Perth exceeded $442,000,000.

558. At all times, Crown Melbourne and Crown Perth understood that Customer 3 was the ultimate beneficial owner of the Meg-Star junket.

559. At all times on and from March 2016 to January 2021, Crown Melbourne and Crown Perth provided table 1 and table 3, s6 designated services to customers through junket programs facilitated by Customer 3.

Particulars

See Customer 3.

560. At all times, Crown Melbourne and Crown Perth were aware that designated services provided through the Meg-Star junket posed higher ML/TF risks, including for the following reasons:

a. Designated services provided by Crown Melbourne and Crown Perth through the Meg-Star junket involved the ML/TF risks as pleaded at paragraph 477.

b. By no later than 15 July 2015, Crown Melbourne was aware that Customer 3, the operator of the Meg-Star junket was closely associated with Suncity, having formerly been an executive at Suncity and acquiring a Suncity entity in 2013.

c. Multiple individuals associated with Customer 3 and the Meg-Star junket were likely to be involved in serious criminal activity, including a junket representative allegedly linked to human trafficking and sex slavery.

Particulars

See Customer 26.

d. Large telegraphic transfers into and out of DAB accounts held by Customer 3, the operator of the Meg-Star junket, including to and from third parties unrelated to the junket.

Particulars

See Customer 3.

e. Large cash transactions involving the Meg-Star junket and its representatives.

Particulars

See Customer 3.

f. Transactions indicative of ML/TF typologies and vulnerabilities involving the Meg-Star junket and its representatives.

Particulars

See Customer 3.

g. Parked monies in DAB accounts held by Customer 3.

Particulars

See Customer 3.

561. From April 2018 to March 2020, Crown Melbourne made a cash administration desk available to the Meg-Star Junket in private gaming rooms.

Particulars

Meg-Star junket staff members dispensed commission chips in exchange for cash to junket players and junket players could deposit cash with the junket.

For the 'soft opening' of the Meg-Star cash administration desk between 9 April 2018 and 14 April 2018, the petty cash limit for the

desk was $500,000 and Crown Melbourne permitted $3 million cash-outs.

Crown Melbourne had limited visibility over transactions through the Meg-Star cash administration desk.

These rooms were not subject to security surveillance.

These rooms were not subject to any AML/CTF controls.

562. Crown Melbourne did not carry out an ML/TF risk assessment in relation to the Meg-Star cash administration desk.

563. The Standard Part A Programs did not include appropriate risk-based controls to identify, mitigate and manage the higher ML/TF risks posed by the matters pleaded at paragraphs 556560 to 562.

Particulars

See paragraphs 478 to 494.

The Neptune junket

564. From 1 March 2016 to 1 November 2020, the Standard Part A Programs did not include appropriate risk-based systems and controls to identify, mitigate and manage the ML/TF risks of designated services provided through the Neptune junket for the reasons pleaded at paragraphs 565 to 569 below.

565. At various times between 2008 to March 2020, Crown Melbourne and Crown Perth had a NONEGPRA with five junket operators who were part of a network of junket operators affiliated with the Neptune Group and Neptune Guangdong Group (the **Neptune junket**).

Particulars

See paragraphs 885 to 887 and Customer 6, Customer 7, Customer 8 and Customer 9.

566. Crown Melbourne and Crown Perth facilitated numerous junket programs with the Neptune junket and with respect to those programs:

a. From 2008 to March 2020, total turnover at Crown Melbourne exceeded $21,764,350,654; and

b. From 2008 to March 2020, total turnover at Crown Perth exceeded $10,392,725,797.

Particulars

See Customer 6, Customer 7, Customer 8 and Customer 9.

567. At all times from March 2016 until January 2021, Crown Melbourne and Crown Perth provided table 1 and table 3, s6 designated services to customers through junket programs facilitated by the junket operators identified at paragraph 565 above.

Particulars

See Customer 6, Customer 7, Customer 8 and Customer 9.

568. At all times, Crown Melbourne and Crown Perth were aware that designated services provided through the Neptune junket posed higher ML/TF risks, including for the following reasons:

a. Designated services provided by Crown Melbourne and Crown Perth through the Neptune junket involved the ML/TF risks as pleaded at paragraph 477;

b. The involvement of Person 3, Person 55 and Customer 6 who were ultimate beneficial owners of the Neptune junket with financial interests in its operations;

Particulars

See paragraph 886 and Customer 6, Customer 7, Customer 8 and Customer 9.

c. Large cash transactions involving the Neptune junket and its representatives;

Particulars

See Customer 6.

d. Large telegraphic transfers into and out of DAB accounts held by Neptune junket operators, including to and from third parties unrelated to the Neptune junket;

Particulars

See paragraph 887 and Customer 6, Customer 7, Customer 8 and Customer 9.

e. DAB account transfers to or from accounts held by Neptune junket operators to or from accounts held by players on Neptune programs, other junket operators and third parties;

Particulars

In December 2016, Customer 6 arranged for the transfer of $4,000,000 from his DAB account to Customer 1's DAB account: see paragraph 905.

f. Amounts owed by Neptune junket operators to Crown Melbourne or Crown Perth being repaid via third party transactions;

Particulars

See Customer 6.

g. Parked monies in the DAB accounts of Neptune junket operators;

Particulars

See Customer 6, Customer 7 and Customer 9.

h. Neptune junket operators being the subject of law enforcement enquiries; and

Particulars

See Customer 6.

i. In 2018, large amounts of cash being carried on Crown private jets by a Neptune junket operator.

Particulars

See Customer 6.

See paragraphs 454 and 491.

569. Having regard to the matters pleaded at paragraphs 565 to 568, the Standard Part A Programs did not include appropriate risk-based controls to identify, mitigate and manage the ML/TF risks of providing designated services through the Neptune junket.

The Chinatown junket

570. From 1 March 2016 to 1 November 2020, the Standard Part A Programs did not include appropriate risk-based systems and controls to identify, mitigate and manage the ML/TF risks of designated services provided by Crown Melbourne and Crown Perth through the Chinatown junket for the reasons pleaded at paragraphs 571 to 580 below.

571. On and from 1 March 2016, Crown Melbourne and Crown Perth had a NONEGPRA with five junket operators who were affiliated with the Chinatown junket (the **Chinatown junket**).

Particulars

See paragraph 967, and Customer 10, Customer 11, Customer 12, Customer 13 and Customer 14.

572. Crown Melbourne and Crown Perth facilitated numerous junket programs for the Chinatown junket, in respect of which:

a. Between 2014 and 2020, turnover for the Chinatown's junket at Crown Melbourne had exceeded approximately $5,975,063,231; and

b. Between 2014 and 2020, turnover for the Chinatown's junket at Crown Perth had exceeded approximately $2,126,626,122.

573. On and from 1 March 2016, Crown Melbourne and Crown Perth were aware of the connection between the Chinatown junket and Person 41, who was an ultimate beneficial owner of the Chinatown junket with financial interests in its operations.

574. At all times on and from March 2016 to January 2021, Crown Melbourne and Crown Perth provided table 1 and table 3, s6 designated services to customers through junket programs operated by the junket operators identified at paragraph 571 above.

Particulars

See Customer 10, Customer 11, Customer 12, Customer 13 and Customer 14.

575. At all times, Crown Melbourne and Crown Perth were aware that designated services provided through the Chinatown junket posed higher ML/TF risks, including for the following reasons:

a. Designated services provided by Crown Melbourne and Crown Perth through the Chinatown junket involved the ML/TF risks as pleaded at paragraph 477;

b. The involvement of Person 41, who was an ultimate beneficial owner of the Chinatown junket with financial interests in its operations, in circumstances where there was law enforcement interest and information publicly available regarding Person 41's alleged criminal activities;

Particulars

See paragraphs 968 and 969.

c. Large cash transactions involving the Chinatown junket operators;

Particulars

See Customer 11, Customer 12, and Customer 14.

d. Large telegraphic transactions into and out of DAB accounts held by Chinatown junket operators including to and from third parties unrelated to the junket;

Particulars

See Customer 11, Customer 12, Customer 13, and Customer 14.

e. DAB account transfers between accounts held by Chinatown junket operators, players on Chinatown junket programs, other junket operators and third parties; and

Particulars

See Customer 11, Customer 12, Customer 13, and Customer 14.

f. Loans granted to Chinatown junket operators were guaranteed by common third parties, including Person 25 and Person 39;

Particulars

See Customer 11, Customer 12, and Customer 13.

576. At no time did Crown Melbourne or Crown Perth conduct appropriate due diligence conducted with respect to Person 41.

577. From March 2016, from time to time, the villa made available to the Customer 2 junket was also used by persons associated with the Chinatown junket.

Particulars

See paragraph 550.

578. Crown Melbourne does not know whether designated services were provided through the villa.

579. Crown Melbourne did not carry out a ML/TF risk assessment in relation to the villa.

580. Junket tour operators associated with the Chinatown junket were provided with access to the Crown private jet in 2016 and 2019.

Particulars

See paragraphs 454 and 491 and 971.

581. The Standard Part A Programs did not include appropriate risk-based controls to identify, mitigate and manage the higher ML/TF risks posed by the matters pleaded at paragraphs 571 to 580.

Particulars

See paragraphs 478 to 494.

The ongoing relationships with persons associated with junkets via the premium player program

582. On 17 November 2020, Crown Resorts announced:

a. it had decided to permanently cease dealing with all junket operators, subject to consultation with State regulators in Victoria, Western Australia and New South Wales; and

b. that it would only recommence dealing with a junket operator if that operator was licensed or otherwise approved by all regulators in the States in which Crown operates.

583. A limited number of former junket representatives have returned to Crown Melbourne and have sought to be regular gaming patrons. These junket representatives have been cleared by Crown Melbourne through the Significant Player Review process and have been permitted to play as regular customers.

The Standard Part A Programs - Transaction monitoring program

584. At all times from 1 March 2016, Crown Melbourne and Crown Perth were required by the Act and Rules to include a transaction monitoring program in their Standard Part A Programs that:

a. included appropriate risk-based systems and controls to monitor the transactions of customers;

b. had the purpose of identifying, having regard to ML/TF risk, any transaction that appears to be suspicious within the terms of s 41 of the Act; and

c. had regard to unusual patterns of transactions, which have no apparent economic or visible lawful purpose.

Particulars

Section 84(2)(c) of the Act, rules 8.1.3, 8.1.4 and rules 15.4 to 15.7 of the Rules.

585. At all times, the Standard Part A Programs included a transaction monitoring program.

a. Clause 12 and Annexure F to the Crown Melbourne Standard Part A Programs set out the transaction monitoring program.

b. Clause 12 of the Crown Perth Standard Part A Programs set out the transaction monitoring program, and incorporated the Crown Perth AML SOP.

c. The Risk Registers also referred to controls relating to monitoring by Crown Melbourne and Crown Perth staff, although the Standard Part A Programs did not refer to these controls as being part of the transaction monitoring program.

Particulars

See paragraph 108.

d. The transaction monitoring programs contained in the Standard Part A Programs comprised of:

i. manual review by the AML/Financial Crime team of the system-generated reports specified in the Standard Part A Program, including those reports identified in the Crown Perth AML SOP;

ii. staff observation on the casino floor and UAR workflows; and

iii. ad hoc exception-based manual reporting (such as review of surveillance or security data).

(the **transaction monitoring programs**)

586. From 1 March 2016 to 1 November 2020, the transaction monitoring programs in the Standard Part A Programs did not comply with the requirements of rules 8.1.3, 8.1.4, 15.4 to 15.7 of the Rules, by reason of the matters pleaded in paragraph 588 to 651.

587. By reason of the matters pleaded in paragraph 586, the transaction monitoring programs did not comply with s 84(2)(c) of the Act during the period from 1 March 2016 to 1 November 2020.

The transaction monitoring programs were not aligned to an appropriate ML/TF risk assessment

588. From 1 March 2016 to 1 November 2020 the transaction monitoring programs in the Standard Part A Programs were not aligned and proportionate to the ML/TF risks reasonably faced by Crown Melbourne and Crown Perth with respect to designated services, having regard to the nature, size and complexity of their businesses and the ML/TF risks reasonably faced.

Particulars

Crown Melbourne and Crown Perth did not appropriately identify and assess the inherent and dynamic ML/TF risks of its designated services.

Rules 8.1.3 and 8.1.4 of the Rules.

By no later than June 2018, the Chief Legal Officer of Crown Resorts, who was also the AMLCO for both Crown Melbourne and Crown Perth, was advised by the Group General Manager AML (Crown Melbourne) that the AML/CTF Program had not been updated for some time; and that key ML/TF risks were not on the Risk Register and do not form part of the transaction monitoring program. See the particulars at paragraph 108.

589. By reason of the matters pleaded at paragraph 588, the transaction monitoring programs in the Standard Part A Programs did not include appropriate risk-based systems and controls to monitor the transactions of customers.

Particulars

Section 84(2)(c) and Rule 15.5 of the Rules.

The transaction monitoring programs did not include appropriate risk-based procedures to monitor for ML/TF typologies and vulnerabilities

590. The ML/TF typologies and vulnerabilities pleaded at paragraph 24 included some indicia of transactions relating to designated services provided by Crown Melbourne and Crown Perth that may have appeared to:

a. be suspicious for the purposes of s 41 of the Act; and/or

b. involve unusual patterns of transactions, which had no apparent economic or visible lawful purpose.

591. In the absence of an appropriate assessment of their ML/TF risks, Crown Melbourne and Crown Perth were unable to design transaction monitoring systems to appropriately detect

transactions that may have been indicative of the ML/TF typologies and vulnerabilities pleaded at paragraph 24.

592. From 1 March 2016 to 1 November 2020, the transaction monitoring programs in the Standard Part A Programs did not include appropriate risk-based procedures to consistently monitor for transactions across all designated services to appropriately detect transactions that may have been indicative of the ML/TF typologies and vulnerabilities pleaded at paragraph 24.

593. At no time did the transaction monitoring programs in the Standard Part A Programs include appropriate risk-based procedures to consistently monitor for transactions of customers indicative of the following possible ML/TF typologies and vulnerabilities:

a. structuring on DAB accounts and safekeeping accounts, including via the Crown Patron account channels;

b. cuckoo smurfing on DAB accounts and safekeeping accounts, including via the Crown Patron account channels;

c. smurfing through third party deposits on DAB accounts and safekeeping accounts, including via the Crown Patron account channels;

d. offsetting on DAB accounts and safekeeping accounts, including through the provision of credit;

e. other transactions on DAB accounts or safekeeping accounts involving third parties who are not the account holder;

f. transaction patterns showing deposits and withdrawals within a short time frame;

g. large holding balances or parked funds on DAB accounts and safekeeping accounts;

h. even money betting and chip dumping;

i. chip or CVI cashing with minimal or no gaming activity;

j. gaming by a customer over time involving high turnover or high losses;

k. bill stuffing with minimal gaming;

l. chip walking/unknown source of chips;

m. jackpot purchases; and

n. loan sharking.

594. The manual transaction monitoring processes in the transaction monitoring programs were not capable of consistently detecting transactions that were indicative of the ML/TF typologies and vulnerabilities (as identified at paragraph 24 above) for the reasons pleaded at paragraphs 601 to 611 below.

595. By reason of the matters pleaded at paragraphs 590 to 594, from 1 March 2016 to 1 November 2020, the transaction monitoring programs in the Standard Part A Programs did not include appropriate risk-based procedures to monitor the transactions of customers:

a. for the purpose of identifying, having regard to ML/TF risk, any transaction that appeared to be suspicious within the terms of s 41 of the Act; and

b. that had regard to unusual patterns of transactions, which had no apparent economic or visible lawful purpose.

Particulars

Section 84(2)(c) and Rules 15.6 and 15.7 of the Rules.

Transactions indicating higher customer risks

596. The Standard Part A Programs specified classes of customers who would not be considered low risk if they engaged in transactional activity that met certain criteria.

597. The transaction monitoring programs did not include or incorporate appropriate risk-based procedures to identify transactions that met the transactional criteria requiring the customer to be risk-rated above low.

Particulars

See paragraph 120j.

For example, there were no transaction monitoring processes to consistently identify transactional criteria that required Crown Melbourne customers to be rated moderate risk by reason of:

- Rated gaming activity where annual loss is between $50,000 and $500,000;
- Multiple cheques issued that were not supported by rated gaming activity; or
- Transactions on deposit accounts not consistent with rated gaming activity – balance under $100,000

Nor were there transaction monitoring processes to consistently identify transactional criteria that required the customer to be rated significant risk by reason of:

- TTRs where annual total loss was in excess of $100,000 which was not supported by rated gaming activity;
- Rated gaming activity where annual win/loss exceeded $500,000;
- Transactions on DAB accounts not consistent with rated gaming activity – balance exceeds $100,000.

There were otherwise no transactional criteria requiring a customer risk rating in Annexure G of the Crown Melbourne Part A Programs or in the Crown Perth AML SOP.

598. By reason of the matters pleaded at paragraph 597, the transaction monitoring programs in the Standard Part A Programs did not include appropriate risk-based systems and controls to monitor the transactions of customers who were not low risk.

Particulars

Section 84(2)(c) of the Act and rule 15.5 of the Rules.

The transaction monitoring programs were manual

599. At all times, the transaction monitoring programs in the Standard Part A Programs were reliant on systems and controls based on:

a. observation and surveillance by front-line staff;

b. manual review by the AML/Financial Crime team of system-generated reports; and

c. ad-hoc exception-based manual reporting.

Particulars

See paragraph 585.

600. At no time did the transaction monitoring programs include or incorporate appropriate risk-based automated monitoring.

601. The manual and observational processes pleaded at paragraph 599 were not capable of detecting suspicious or unusual patterns of transactions or behaviours across complex transaction chains involving multiple designated services.

Particulars

See paragraphs 18 and 19.

The manual and observational transaction monitoring processes were focussed on individual transactions, and were not capable of assessing the complex transaction chains within which they sat.

602. The transaction monitoring program did not include appropriate risk based systems and controls to monitor transactions on EGMs and ETGs.

Particulars

By no later than June 2018, the Chief Legal Officer of Crown Resorts, who was also the AMLCO for both Crown Melbourne and Crown Perth, was advised by the Group General Manager AML (Crown Melbourne) that that there was no direct monitoring of transactional activity on EGMs and ETGs, other than as part of surveillance.

The Chief Legal Officer/AMLCO was advised that this meant EGMs and ETGs were vulnerable to the ML/TF typology of bill stuffing.

The Group General Manager AML recommended that the absence of direct monitoring of EGMs and ETGs should be taken to Board level for its consideration as to its comfort level.

603. The systems-generated and the ad-hoc exception based manual reports were not capable of consistently and fully identifying across all designated services:

a. transactions that may have had indicia of the ML/TF typologies and vulnerabilities (as identified at paragraph 24 above);

b. transactions that may be suspicious for the purposes of s41 of the Act; and

c. unusually large or unusual patterns of transactions, which had no apparent economic or visible lawful purpose.

Particulars

Rules 15.6 and 15.7 of the Rules.

For example:

The multiple ‘buy-in’ reports that were to be run once weekly were not capable of identifying structuring of transactions.

The telegraphic transfer report was run on an ad hoc basis at Crown Melbourne and was required to be run daily at Crown Perth. It needed to be reviewed on a line-by-line basis, without any tools and was a laborious process.

Designated services provided through EGMs and through poker games were not recorded in daily summary reports.

The gaming trends report, which was intended to identify gaming trends, concession status and DAB accounts with balances of $2,000 or more with no activity, was only run yearly. There were no criteria against which to review this report and its purpose was not clear.

The manual reporting processes in the Standard Part A Programs for monitoring foreign exchange were only to be applied ‘as required’ and appeared only to apply to exchanges of physical foreign currency.

604. The transaction monitoring programs did not provide adequate review criteria for the systems-generated and the ad-hoc exception based manual reports.

605. The transaction monitoring programs did not provide adequate guidance on how to identify unusually large transactions.

Particulars

Rules 15.6 and 15.7 of the Rules.

Large transactions, including large cash transactions or balances, were to be identified through manual transaction monitoring, surveillance, and by staff observation of customer behaviour.

'Large' in relation to these risks was not a defined term, and was based on a range of factors, including Crown Melbourne staff knowledge of the customer and their usual behaviour and gaming activity.

In particular, the perception of whether a transaction was 'large' was viewed through the lens of whether the transaction was unusual for that particular customer, or category of customer.

In the absence of appropriate criteria for identifying unusually large transactions and in the absence of information about source of wealth or funds, it was not possible to consistently identify activity that lacked an apparent economic or visible lawful purpose.

606. From time to time, some Crown Melbourne and Crown Perth staff were provided with training related to AML/CTF, including through online training modules.

607. Frontline staff and staff reviewing systems-generated or exception-based reports were unable to appropriately monitor the transactions of customers for the purposes of the transaction monitoring program because they did not receive adequate ML/TF risk awareness training.

Particulars

Frontline staff were staff with customer facing roles relating to table games, gaming machines, surveillance, security, Cage functions and VIP.

608. The staff identified at paragraph 607 did not receive adequate ML/TF risk awareness training for the following reasons:

a. As Crown Melbourne and Crown Perth did not carry out appropriate ML/TF risk assessments, their risk awareness training did not adequately cover the ML/TF risks reasonably faced with respect to designated services.

b. The training modules did not cover all of the ML/TF typologies and vulnerabilities pleaded at paragraph 24 above.

c. To the extent the training modules did include a reference to the ML/TF typologies or vulnerabilities, they did not provide adequate explanation or guidance.

d. Prior to 2019, the training modules did not cover key risks and risk factors, such as those related to junkets and the elevated risks of certain customer classes, jurisdictions, products and channels.

e. The training modules did not address the ML/TF risks of table 1 s6 financial services, including remittance services or loans.

f. Key ML/TF risks and typologies that were missing from the training modules included cuckoo smurfing and third party transactions.

g. The typology of structuring was referenced at a high level, but did not address structuring by way of cash deposits into DAB accounts and safekeeping accounts through Crown Patron accounts.

h. ML/TF risks and typologies such as bill stuffing and refining were included in training but not meaningfully addressed.

i. The Crown Melbourne CTRM, the key resource upon which the manual transaction monitoring program relied, was not provided with adequate training to enable the functions to be properly carried out.

j. The Crown Perth AML Officer or Legal Officer – AML was responsible for actioning or responding to manual transaction monitoring alerts. The persons occupying those roles did not receive adequate training to enable that function to be properly carried out.

Particulars

Part 8.2 of the Rules.

609. The resourcing of the AML/Financial Crime functions did not support the consistent generation, review and actioning of systems-generated or exception-based reports as required by the transaction monitoring program.

Particulars

Until July 2018, only one staff member, the Crown Melbourne CTRM, was responsible for actioning transaction monitoring reports at Crown Melbourne. From July 2018 to November 2020,

the Financial Crime team (comprised of 5 persons as at January 2020) had this responsibility.

In May 2018, AUSTRAC expressed concern to Crown Melbourne that, despite the high volume and value of transactions conducted at Crown Melbourne there were only two staff, equating to approximately 1.5 full time equivalent staff that had day-to-day responsibility for overseeing Crown Melbourne's transaction monitoring and reporting obligations.

The Crown Perth AML Officer or Legal Officer – AML were responsible for actioning transaction monitoring reports. At most times from 1 March 2016, there was a single Crown Perth AML Officer responsible for the key roles that were expressly referred to in each version of the Crown Perth Standard Part A Program, with support from the AMLCO.

Many of the systems-generated reports and ad hoc exception based reports contained high volumes of data that were laborious to review. Resourcing of the AML/Financial Crime roles responsible for transaction monitoring was not adequate to review this volume of data with the frequency required by the transaction monitoring programs.

610. The review of surveillance and security data at Crown Melbourne was ad-hoc, manual and exception-based.

Particulars

Surveillance and security failed to detect highly suspicious cash transactions in private gaming rooms.

611. Transaction monitoring reliant upon manual processes was not appropriate for businesses of the size, nature and complexity of Crown Melbourne and Crown Perth.

Particulars

Rule 8.1.3 of the Rules.

612. For the reasons pleaded at paragraphs 601 to 611, the systems and controls pleaded at paragraph 599 were not appropriate risk-based systems and controls that were capable of consistently identifying transactions that may have:

a. appeared to be suspicious for the purposes of s41 of the Act; or

b. involved unusual patterns of transactions, which had no apparent economic or visible lawful purpose.

Particulars

Rules 8.1.3, 8.1.4, 8.2, 15.5, 15.6 and 15.7 of the Rules.

In September 2012, AUSTRAC first recommended to Crown Melbourne that it consider automated monitoring. AUSTRAC made this recommendation to Crown Melbourne again in August 2014 and in May 2018.

In 2012, AUSTRAC recommended to Crown Perth that they consider implementing a more sophisticated automated transaction monitoring program to widen current monitoring and incorporate cross referencing with customer occupation information, noting the volume of transactions.

In June 2018, the Chief Legal Officer of Crown Resorts, who was also the AMLCO for both Crown Melbourne and Crown Perth, was briefed by the Group General Manager AML on the need to investigate automation of elements of transaction monitoring program.

Work did not start on the project to build an automated transaction monitoring framework until 2019 and it did not go live until February 2021, at which point it continued to operate in parallel with Crown Melbourne's manual monitoring system. The uplift is ongoing.

The transaction monitoring programs were not supported by appropriate information management systems

613. From 1 March 2016 to 1 November 2020, transaction monitoring by Crown Melbourne and Crown Perth through systems-generated reports and exception-based reports was reliant upon data entered into SYCO.

614. At all times, SYCO was subject to the following limitations:

a. The entry of transactional data into SYCO, was largely a manual process which was not always complete and was subject to human error.

Particulars

For example, see paragraph 635.

b. The entry of transactional data into ATOM, which fed table games data into SYCO, was largely a manual process which was not always complete and was subject to human error, as pleaded at paragraph 615.

c. SYCO did not contain a full record of all transactions provided by Crown Melbourne and Crown Perth with respect to designated services, including as pleaded at paragraphs 616, 619 and 648.

d. SYCO transaction records were not always consistently linked to a customer, for the reasons pleaded at paragraphs 619 to 624.

ATOM

615. Dealers at tables were responsible for entering data into ATOM in relation to table 6 and 9, table 3 designated services. Dealers were unable to capture all transactions at table games relating to the provision of these designated services.

Particulars

Given the role of Dealers in running the games, and that Table Games Area Managers monitored multiple tables, and that not all bets, winnings, and losses were entered, the accuracy of ratings from table games recorded against a customer's PID could not be guaranteed.

Transactions under $10,000

616. At all times, SYCO contained limited records of transactions under $10,000 conducted by Crown Melbourne and Crown Perth unless the customer elected to play carded (that is, against a Crown Rewards membership):

a. Cash transactions under $10,000 for non-deposit account customers were not recorded in SYCO.

b. Gaming buy-in and pay-out transactions were manually entered into SYCO only if they were $10,000 or above.

c. Exchanges of money for chips and vice-versa for less than $10,000 were not entered into SYCO.

d. Payment of winnings or accumulated credits less than $10,000 from an EGM were not entered into SYCO.

617. By reason of the matters pleaded at paragraph 616:

a. the systems-generated and exception-based reports did not appropriately cover transactions under $10,000; and

b. monitoring of table 3 designated services under $10,000 was limited to the observations of Crown Melbourne and Crown Perth staff.

Particulars

By no later than June 2018, the Chief Legal Officer of Crown Resorts, who was also the AMLCO for both Crown Melbourne and Crown Perth, was advised by the Group General Manager AML (Crown Melbourne) that that there were no specific controls at Crown Melbourne to monitor for transactions under $10,000 for certain risks, resulting in vulnerability to structuring. For example, other than observational monitoring, there was no monitoring for chip for cash transactions below $10,000 at the Cage.

618. By reason of the matters pleaded at paragraph 617, the transaction monitoring program was unable to appropriately monitor:

a. for transactions that were structured to avoid reporting of cash transactions of $10,000 or above; and

b. a customer's turnover that exceeded $10,000 in any one session of play, where buy-in or cash-out transactions were under $10,000.

Uncarded transactions

619. Customers of Crown Melbourne and Crown Perth could elect to play **uncarded**. That is, a customer could buy-into or enter a table game or EGM within the meaning of item 6, table 3, s6 without swiping a Crown Rewards card.

620. Crown Melbourne and Crown Perth permitted uncarded customers to buy-into a table game or EGM for amounts of $10,000 or more.

621. Uncarded transactions were not recorded in SYCO as against a customer's profile.

Particulars

Uncarded plays recorded on ATOM were used to create a customer **rating** and were not linked to any customer data or PID number.

Uncarded Ratings were typically used for accounting purposes to understand and track fluctuations in the table float.

Uncarded ratings would only be recorded if a dealer or area manager noticed play on a gaming table that warranted recording for accounting purposes.

See paragraph 615.

622. The transaction monitoring programs were unable to attribute uncarded transactions to individual customers.

Particulars

This limited Crown Melbourne's and Crown Perth's ability to identify unusual or suspicious matters, for example, buy-ins with little or no corresponding gaming activity.

623. At all times, records relating to customers (including KYC information and risk profile information) were dispersed across systems other than SYCO.

Particulars

See paragraphs 55 to 67.

624. Crown Melbourne and Crown Perth gave customers multiple gaming accounts, across multiple reference numbers and sometimes in different customer names or under pseudonyms.

Particulars

See paragraph 680 below.

625. By reason of the matters pleaded at paragraphs 619 to 624 the transaction monitoring programs were unable to consistently attribute transactions to individual customers.

626. A reporting entity cannot consistently identify transactions that may be:

a. suspicious for the purposes of s41 of the Act; or

b. unusually large or involve unusual patterns with no apparent economic or visible lawful purpose

in the absence of appropriate KYC information relating to the customer conducting the transaction.

627. By reason of the matters pleaded at paragraphs 613 to 626, from 1 March 2016 to 1 November 2020, the transaction monitoring programs in the Standard Part A Programs were not aligned to the nature, size and complexity of Crown Melbourne's and Crown Perth's business, having regard to the ML/TF risks they reasonably faced.

Particulars

Rule 8.1.3 of the Rules.

628. By reason of the matters pleaded at paragraphs 613 to 627, from 1 March 2016 to 1 November 2020, the transaction monitoring programs in the Standard Part A Programs did

not include appropriate risk-based systems and controls to monitor the transactions of customers.

Particulars

Rules 8.1.3, 8.1.4, 15.5, 15.6 and 15.7 of the Rules.

The transaction monitoring program was not capable of appropriately monitoring financial services or gaming account transactions

629. From 1 March 2016 to 1 November 2020, the transaction monitoring program in the Standard Part A Programs did not include appropriate risk-based systems and controls to monitor the transactions of customers in relation to:

a. items 6 and 7, table 1, s6 designated services with respect to loans or credit;

b. items 13, table 3, s6 designated services with respect to gaming accounts; and

c. items 31 and 32, table 1, s6 designated services with respect to remittance

by reason of the matters pleaded at paragraphs 630 to 642.

Particulars

Rules 8.1.3, 15.5, 15.6 and 15.7 of the Rules.

Loans or credit

630. From 1 March 2016 to 1 November 2020, the transaction monitoring programs in the Standard Part A Programs did not include any risk-based systems and controls to monitor the transactions of customers with respect to designated services under items 6 and 7 of table 1, s6 of the Act.

Particulars

The transaction monitoring programs did not include any processes that were expressed to apply to items 6 and 7, table 1, s6 designated services.

The transaction monitoring program did not include or incorporate any processes that were capable of monitoring items 6 and 7, table 1, s6 designated services, having regard to the ML/TF risks pleaded at paragraph 394.

The Credit Control and VIP Finance teams, who facilitated the loans or credit business did not monitor for transactions that may be suspicious or unusual, having regard to ML/TF risks.

See paragraphs 588 to 628.

DAB, safekeeping and Card Play Extra accounts

631. From 1 March 2016 to 1 November 2020, the transaction monitoring programs in the Standard Part A Programs did not include appropriate risk-based systems and controls to monitor the transactions of customers with respect to designated services under items 11 and 13 table 3, s6 of the Act, by reason of the matters pleaded at paragraphs 632 to 638 below.

Particulars

Items 11 and 13, table 3, s6 designated services were provided with respect to DAB, safekeeping and Card Play Extra accounts.

See paragraphs 588 to 628.

632. The transaction monitoring programs did not include appropriate risk-based systems and controls to consistently monitor the provision of items 11 and 13, table 3, s6, designated services to customers for the purposes of identifying any transactions that may be suspicious or unusual, having regard to:

a. The ML/TF risks pleaded at paragraph 219 with respect to DAB accounts and safekeeping accounts; and

b. The ML/TF risks pleaded at paragraph 279 with respect to Card Play Extra accounts.

633. The transaction monitoring programs did not include appropriate risk-based procedures to consistently monitor DAB accounts and safekeeping accounts for item 13, table 3, s6 transactions potentially indicative of the ML/TF typologies pleaded at subparagraphs 593 a to g.

634. The manual reporting processes in the transaction monitoring programs that applied to telegraphic transfers to and from DAB accounts and safekeeping accounts were not capable of consistently identifying any transactions that may have been suspicious or unusual, having regard to the ML/TF risks pleaded at paragraph 219, for the following reasons:

a. The transaction monitoring programs in the Crown Melbourne Standard Part A Programs required manual reporting for telegraphic transfers on an ad hoc basis only.

b. Crown Melbourne had no written guidance on what factors would trigger an ad hoc review; who would conduct an ad hoc review; or the criteria for any ad hoc review.

c. The Crown Perth AML SOP required daily review of telegraphic transfers.

d. Crown Perth had no written guidance on the criteria for review of such transfers.

635. At no time did the transaction monitoring programs include appropriate risk-based systems and controls to monitor the transactions of customers in relation to designated services on DAB accounts and safekeeping accounts under item 13 table 3, s6 of the Act through the Crown Patron account channel, including by reason of the following matters:

a. When a customer deposited funds into a Crown Patron account, Crown Melbourne and Perth Cage staff would enter those deposits into the customer's DAB account or safekeeping account maintained on SYCO.

b. Where multiple deposits had been made by or for a customer into a Crown Patron account, Crown Melbourne and Crown Perth Cage staff had a practice of aggregating those deposits into a single credit entry on the customer's DAB account.

c. This practice was in place at Crown Melbourne and Perth all relevant times until 2020.

d. The AML/Financial Crime teams relied on the SYCO record for transaction monitoring and customer due diligence.

e. Multiple deposits could be indicative of structuring (if cash under $10,000) or cuckoo smurfing or both.

f. By aggregating deposits on the SYCO record, the AML/Financial Crime Teams were unable to identify patterns of transactions that may have been indicative of money laundering.

g. The practice of aggregation meant unusual and suspicious activity was not identified by Crown Melbourne and Crown Perth.

h. Review of payment flows through Crown Patron accounts by the Credit Control or VIP Finance team was manual and not subject to any AML/CTF criteria.

Particulars

At all times until 2020, multiple deposits to the Southbank and Riverbank accounts were aggregated.

Crown Melbourne and Crown Perth failed to apply appropriate second line assurance and third line audit to DAB accounts, such that the practice of aggregation was not detected until 2020.

The unchecked, systemic and longstanding aggregation process actively and necessarily facilitated money laundering.

External AML/CTF experts have identified numerous transactions on DAB accounts and safekeeping accounts that were remitted through the Southbank and Riverbank accounts which were assessed as indicative of money laundering.

636. The manual reporting processes in the transaction monitoring programs that applied to transfers from one customer's DAB account to another customer's DAB account were not capable of consistently identifying any transactions that may have been suspicious or unusual, having regard to the ML/TF risks pleaded at paragraph 219, for the following reasons:

a. The transaction monitoring programs in the Crown Melbourne Standard Part A Programs provided that, as required, fund transfers from one customer's DAB account to another customer's DAB account would be reviewed.

b. Crown Melbourne had no written guidance on what factors would trigger a review; who would conduct the review; or the criteria for any review.

c. The Crown Perth AML SOP required weekly review of 'intra-patron transfers' to identify unusual patterns of activity.

d. Crown Perth had no written guidance on the criteria for any such review.

637. The transaction monitoring programs in the Standard Part A Programs did not refer to Card Play Extra accounts.

638. The transaction monitoring programs in the Standard Part A Programs did not include any processes to monitor cash deposits and withdrawals through the Card Play Extra accounts.

Items 31 and 32, table 1, s6 remittance services

639. From 1 March 2016 to 1 November 2020, the transaction monitoring programs in the Standard Part A Programs did not include appropriate risk-based systems and controls to monitor the transactions of customers with respect to designated services under items 31

and 32 table 1, s6 of the Act, by reason of the matters pleaded at paragraphs 640 to 642 below.

Particulars

See paragraphs 588 to 628.

640. The transaction monitoring programs did not include appropriate risk-based systems and controls to consistently monitor the provision of items 31 and 32, table 1, s6 designated services to customers for the purposes of identifying any transactions that may be suspicious or unusual, having regard to the ML/TF risks pleaded at paragraph 420.

641. For the reasons pleaded at paragraph 634 to 636, remittance transactions (being items 31 and 32, table 1, s6 designated services) that were facilitated through DAB accounts and safekeeping accounts were not subject to appropriate risk-based monitoring under the transaction monitoring programs.

642. The manual reporting processes in the transaction monitoring programs were not capable of consistently monitoring item 31 and 32, table 1, s6 designated services for the purposes of identifying suspicious or unusual transactions.

Transactions facilitated through junkets

643. From 1 March 2016 to 1 November 2020, the transaction monitoring program in the Standard Part A Programs did not include appropriate risk-based systems and controls to monitor the transactions of customers receiving designated services through junket channels, for the reasons pleaded at paragraphs 644 to 649.

Particulars

Rules 8.1.3, 15.5, 15.6 and 15.7 of the Rules.

See paragraphs 588 to 628.

644. The transaction monitoring programs did not include appropriate risk-based systems and controls to consistently monitor the provision of designated services to customers through junket channels for the purposes of identifying any transactions that may be suspicious or unusual, having regard to the ML/TF risks pleaded at paragraph 477.

Particulars

Customers who received designated services through junket channels were subject to the same standard monitoring applied to all other customers.

645. The transaction monitoring programs did not include appropriate risk-based systems and controls to monitor transactions relating to table 1, s6 designated services (loans and remittance) provided through junket channels.

Particulars

Any review of junket transactions by VIP Finance and/or the Credit Control team, or the Crown Perth Cage, was not for the purpose of identifying, mitigating or managing ML/TF risks.

See paragraphs 630 and 639 to 642.

646. The transaction monitoring programs did not include appropriate risk-based systems and controls to monitor deposits to DAB accounts or safekeeping accounts through Crown Patron accounts on behalf of junket operators or players.

Particulars

See paragraph 635.

647. The transaction monitoring programs did not include appropriate risk-based systems and controls to monitor the transactions of customers relating to designated services facilitated through junket channels in private gaming rooms.

Particulars

Monitoring of transactions within private gaming rooms was largely limited to staff observation and surveillance.

CCTV or surveillance could not be used, on its own, to effectively monitor the transactions of customers in private gaming rooms for known ML/TF risks.

648. The transaction monitoring programs were not able to fully monitor designated services provided through junket channels because Crown Melbourne and Crown Perth did not make or keep appropriate records of transactions conducted by key players.

Particulars

See paragraph 477.

The gaming activity of individual players on junkets recorded on SYCO was reliant on junket operator records.

Crown Melbourne and Crown Perth did not have appropriate systems and controls in place to ensure that junket operator records reliably attributed play to key players.

Crown Melbourne made no record of cash transactions conducted in the private gaming rooms made available to the Suncity Junket, including through the Suncity cash administration desk and as such was unable to apply appropriate transaction monitoring.

649. The manual processes in the transaction monitoring program and in the Risk Registers were not appropriate risk-based controls for monitoring transactions relating to designated services provided through the junket channel.

Particulars

The Risk Register required junket operator, junket representative and key play behaviour and accounts to monitored by the AML team and by the Credit Control (in identified circumstances). This was not an appropriate risk-based transaction monitoring control.

Surveillance and security staff trained to identify and report suspicious behaviour was also identified as a control. This was not an appropriate risk-based transaction monitoring control.

At Crown Melbourne, the transactional activity of junket players who transacted $50,000 or more were to be subject to ad hoc manual

review by the CTRM. There was no guidance as to when an ad hoc review would be triggered; nor were there criteria for this review. The process was manual and laborious.

The Crown Melbourne transaction monitoring program did not include appropriate risk-based systems and controls to monitor transactions through the HCT channel

650. From 1 March 2016 to October 2016, the transaction monitoring program in Crown Melbourne's Standard Part A Program did not include appropriate risk-based systems and controls to monitor the transactions of customers who received designated services through the HCT channel:

a. HCT funds became commingled with other funds and transactional activity at the point it was credited into the customer's DAB account.

b. No monitoring was conducted specifically on the origin of the HCT funds.

c. As a result, Crown Melbourne was unable to identify, mitigate and manage unusual or suspicious activity connected to the HCT channel.

d. None of the data fields in SMR records reviewed by an external auditor identified any reference to the HCT activity.

Particulars

Rules 8.1.3, 15.5, 15.6 and 15.7 of the Rules.

The transaction monitoring programs did not include appropriate assurance processes

651. The transaction monitoring programs in the Standard Part A Programs did not include or incorporate appropriate risk-based systems and controls for assurance.

a. There were no quality assurance processes at the operational level, such a 'four eye check' or peer review, to confirm that processes in the transaction monitoring program (such as review of manual reports) were being applied correctly.

b. There were no controls for reviewing whether transaction monitoring criteria or reporting were capturing behaviours of concern, including new or changed behaviours.

c. There were no controls to ensure that updates to ML/TF risk assessments or material changes to ML/TF risk profile were recognised in the transaction monitoring programs.

d. There was no periodic review of the overall transaction monitoring framework to ensure that escalation and decision-making processes were effective and being consistently applied, and that the transaction monitoring programs were properly aligned to other AML/CTF systems and controls.

Particulars

Sections 84(2)(a) and (c) and rules 8.1.3 and 15.5 of the Rules.

The Standard Part A Programs - Enhanced customer due diligence program

652. At all times from 1 March 2016, Crown Melbourne and Crown Perth were required by the Act and Rules to:

a. include an enhanced customer due diligence (**ECDD**) program in its Part A Program that complies with the requirements of the Rules;

b. apply the ECDD program when:

i. Crown Melbourne or Crown Perth determines under its risk-based systems and controls that the ML/TF risk is high;

ii. a designated service is being provided to a customer who is or who has a beneficial owner who is, a foreign PEP; or

iii. a suspicion has arisen for the purposes of s41 of the Act; and

(the **ECDD triggers**).

c. include appropriate risk-based systems and controls in their ECDD program so that, in cases where one or more of the circumstances identified in paragraph b above arises, Crown Melbourne or Crown Perth was required to undertake measures appropriate to the circumstances, including the range of measures in rule 15.10 of the Rules (**ECDD measures**), including but not limited to:

i. clarify or update KYC information already collected from the customer;

ii. clarify or update beneficial owner information already collected from the customer;

iii. obtain any further KYC information or beneficial owner information, including, where appropriate, taking reasonable measures to identify the customer's source of wealth and funds and the beneficial owner's source of wealth and funds;

iv. undertake a more detailed analysis of the customer's source of wealth and funds and the beneficial owner's source of wealth and funds;

v. undertake more detailed analysis and monitoring of the customer's transactions;

vi. seek senior management approval for continuing a business relationship with the customer and whether a designated service should continue to be provided to a customer; and

vii. consider whether a transaction or particular transactions should be processed.

Particulars

Section 84(2)(c) of the Act and rules 1.2.1 (definition of KYC information), 8.1.3 and 8.1.4, 15.8 to 15.11 of the Rules.

653. An ECDD Program must include appropriate systems and controls to apply ECDD measures to customers falling within rules 15.9(1) and (2) from time to time, on a risk-basis.

Particulars

Sections 36, 84(2)(a) and (c) of the Act; and rules 8.1.3, 8.1.4, 8.1.5, 15.9 and 15.10 of the Rules.

654. At all times, the Crown Melbourne and Crown Perth Standard Part A Programs included an enhanced customer due diligence Program (**the ECDD Programs**).

a. Clause 15 and Annexure H to the Crown Melbourne Standard Part A Program set out the ECDD Program and provided that it comprised:

i. Transaction Monitoring Program (Annexure F);

ii. Risk Rating (Annexure G); and

iii. Crown Melbourne's AML/CTF Guidelines.

(the **Crown Melbourne ECDD Programs**).

b. Clause 15 of the Crown Perth Standard Part A Program set out the ECDD Program; and the Crown Perth AML SOP also required various checks to be conducted upon an ECDD trigger (the **Crown Perth ECDD Programs**).

655. By reason of the matters pleaded in paragraph 657 to 683, the ECDD Programs in the Standard Part A Programs did not comply with rules 15.8 to 15.11 of the Rules from 1 March 2016 to 1 November 2020.

656. By reason of the matters pleaded in paragraph 655, the Part A Programs did not comply with s 84(2)(c) of the Act from 1 March 2016 to 1 November 2020.

Systems and controls to determine when a customer should be referred for ECDD

657. From 1 March 2016 to 1 November 2020, the ECDD Programs did not include appropriate systems, controls and procedures for Crown Melbourne or Crown Perth to apply ECDD to customers, as and when appropriate on a risk-basis, who were:

a. determined to pose high ML/TF risk;

b. foreign PEPs or had a beneficial owner who was a foreign PEP; or

c. the subject of a suspicion that had arisen for the purposes of s41 of the Act

for the reasons set out at paragraphs 658 to 664 below.

658. At all times, the Crown Melbourne ECDD Programs required the following types of customers to have an automatic high risk rating:

a. customers known to have engaged in ML/TF;

b. customers known to be a foreign PEP; or

c. a company.

Particulars

Annexure G, Appendix 3, of the Crown Melbourne Standard Part A Programs

659. At all times, the Crown Perth ECDD Programs required customers known to have engaged in ML/TF to have an automatic high risk rating.

Particulars

Appendix B of the Crown Perth Standard Part A Programs.

Customers who were automatically high risk

660. From 1 March 2016 to 1 November 2020, the ECDD Programs did not include appropriate systems, controls and procedures for Crown Melbourne or Crown Perth to identify customers who were required to have an automatic high risk rating, and to escalate them for ECDD as and when appropriate on a risk basis, for the following reasons:

a. Screening through World-Check/Dow Jones was relied upon to initially identify customers with criminal records or who were PEPs.

b. Screening processes were limited by reason of the matters pleaded at paragraph 120.

c. The CTRM (in Melbourne) or the Legal Officer - AML (in Perth) could add an alert to a customer's SYCO profile when, through screening or other means, the CTRM or AMLCO became aware that the customer was:

   i. a PEP;

   ii. the customer was charged or convicted of a criminal offence;

   iii. the customer was a citizen of a sanctioned jurisdiction;

   iv. the customer was the subject of a Law Enforcement Agency request; or

   v. Crown Melbourne or Crown Perth became aware of adverse media in respect of the customer.

d. The process for creating SYCO alerts was ad hoc, manual, not subject to appropriate criteria and not supported by adequate resources.

e. At both Crown Melbourne and Crown Perth, a daily SYCO Alert Report was required to be generated by the CTRM or the Legal Officer - AML. The report included the customer's PID, name, all activities that occurred on the customer's account the preceding day, and the amount and time of each recorded transaction (if any).

f. The review of the daily SYCO Alert Report was manual, not subject to appropriate criteria and not supported by adequate resources. This process was not capable of consistently identifying customers that should have been rated high risk and who should have been referred for ECDD.

g. As the Part B Programs provided for 'safe-harbour' ACIP only, customers who should have been automatically rated high were not capable of being consistently identified and referred for ECDD.

h. The transaction monitoring programs were not capable of consistently identifying and escalating customers engaging in unusual or suspicious transactions.

i. There were no processes in place for the Credit/VIP International teams to refer customers to the AML/Financial Crime teams for ECDD when, during the course of a credit risk assessment, matters relevant to ML/TF risk were identified.

j. There were no processes to consistently identify when customers would be referred to senior management for approval with respect to the ongoing business relationship or the processing of transactions.

Particulars

See paragraph and 668.

k. There were no processes to consistently refer customers to the POI Committee (as to which see paragraph 672) for review where relevant information had been received from law enforcement.

Particulars

Rule 15.9(1) of the Rules.

See paragraph 653.

Customers who had been rated high risk

661. From 1 March 2016 to 1 November 2020, the ECDD Programs did not include appropriate systems, controls and procedures for Crown Melbourne or Crown Perth to escalate customers who had been rated high risk for ECDD as and when appropriate on a risk basis, for the following reasons:

a. Under the Crown Melbourne Standard Part A Programs, the CTRM (or later the AML team) reviewed the risk ratings of customers rated 'Significant' and 'High' at least once every two years.

b. That review considered any continued law enforcement interest in the customer, whether any SMRs had been submitted in relation to the customer, and the level of gaming activity or financial transactions for the customer.

c. This process was too infrequent and did not involve a referral of the customer for full ECDD.

d. The daily SYCO Alert report was not capable of consistently identifying high risk customers who were required to be subject to ECDD for the reasons pleaded at paragraph 660.

e. There were no other processes in the ECDD Programs to consistently escalate customers that had been rated high risk for appropriate ECDD, to meet the requirements of rules 15.9 and 15.10.

Particulars

Rule 15.9(1).

See paragraph 653.

See paragraphs 660c to k.

Customers considered low risk by default or rated less than high risk

662. The Standard Part A and Part B Programs were not capable of identifying and escalating customers who presented high risks, but who were yet to be rated high risk by Crown Melbourne or Crown Perth, for the following reasons.

a. The processes for identifying and escalating customers who were not low risk by default were inadequate, for the reasons pleaded at paragraph 120.

b. As the Standard Part B Programs provided for 'safe-harbour' ACIP only, customers who should have been automatically rated high risk were not capable of being consistently identified and referred for ECDD.

Particulars

See paragraphs 118 and 119.

c. There were no appropriate risk-based processes to determine in what circumstances further KYC information should be collected in respect of a customer to enable the review and update of KYC information for ongoing customer due diligence purposes: rule 15.2 of the Rules.

d. There were no appropriate risk-based processes for keeping, updating and reviewing documents, data or information collected under an ACIP, particularly in relation to high risk customers.

Particulars

Rule 15.3 of the Rules.

e. The transaction monitoring programs were not capable of consistently identifying and escalating customers engaging in unusual or suspicious transactions, in particular:

i. The transaction monitoring programs were not capable of identifying and escalating customers who moved money through complex transaction chains involving both table 1 (financial) and table 3 (gaming) s6 designated services.

ii. The transaction monitoring programs were not capable of identifying and escalating customers whose transactions involved third parties or agents.

iii. The transaction monitoring programs had limited application to customers who were transacting under $10,000, who were uncarded (see paragraph 619) and who had not been the subject of ACIP. It had limited capacity to identify customers engaging in structuring.

iv. Dispersed data sources for customer information limited Crown Melbourne's and Crown Perth's ability to understand a customer's transactional activity and to determine whether any particular activity was unusual.

v. There were no procedures in the transaction monitoring program requiring escalation of customers where transactions indicating high risk had been detected.

Particulars

Rule 15.9(1) of the Rules.

Foreign PEPs

663. From 1 March 2016 to 1 November 2020, the ECDD Programs did not include appropriate systems, controls and procedures for Crown Melbourne or Crown Perth to consistently identify and escalate customers who were foreign PEPs for ECDD as and when required on a risk basis, for the following reasons:

a. Screening for PEPs was inadequate for the reasons pleaded at paragraph 120.

b. There were no processes in place for the Credit/VIP International teams to refer customers to the AML/Financial Crime teams for ECDD when, during the course of a credit risk assessment, the customer was identified as a foreign PEP.

c. Whilst the ECDD Programs stated that certain ECDD measures would be undertaken with respect to foreign PEPs, there were no processes for Crown Melbourne or Crown Perth to appropriately and consistently:

i. undertake more detailed analysis of the foreign PEP's KYC information, including where appropriate, taking reasonable measures to identify the customer's source of funds and wealth; and

ii. ensure senior management approval would be sought for a continuing business relationship with the foreign PEP and whether a designated service should continue to be provided to the foreign PEP.

d. The Crown Melbourne ECDD Programs provided that for the purposes of seeking Senior Management approval, the AML Team will be authorised to make a decision in the first instance after consideration of all available information and having regard to the ML/TF risk. The ECDD Programs provided that the AML Team could refer the final decision to the AMLCO and other members of senior management where appropriate, but there was no guidance or criteria relating to this process. This was not an appropriately risk-based procedure, having regard to the nature, size and complexity of Crown Melbourne's business.

Particulars

Rules 8.1.3, 15.9(2) and 15.11 of the Rules.

See paragraphs 660c to f.

Customers in respect of whom a s41 suspicion had arisen

664. From 1 March 2016 to 1 November 2020, the ECDD Programs did not include appropriate systems, controls and procedures for Crown Melbourne or Crown Perth to escalate customers for appropriate ECDD when a s41 suspicion arose.

a. UAR workflows (via the internal SMR form) were not clearly mapped to ECDD.

b. The CTRM (or Financial Crime team) (in Melbourne) or the AMLCO (in Perth) were expected to initiate ECDD at the same time that an SMR was reported. However:

i. in the absence of appropriate guidance, criteria and resources, there was little to no review of the customer beyond that involved in submitting the SMR; and

ii. in substance, there was no process to conduct appropriate risk-based ECDD when a s41 suspicion arose.

Particulars

Rule 15.9(3) of the Rules.

Systems and controls to determine what ECDD measures would be undertaken

665. From 1 March 2016 to 1 November 2020, the ECDD Programs did not include systems and controls to carry out appropriate risk-based ECDD measures once a customer had been referred for ECDD, for the reasons pleaded at paragraphs 666 to 683.

No procedures or guidance appropriately addressing the suite of ECDD measures specified by the Rules

666. From 1 March 2016 to 1 November 2020, the ECDD Programs did not include or incorporate appropriate procedures or guidance on the suite of risk-based ECDD measures to be applied by Crown Melbourne or Crown Perth for the following reasons:

a. The ECDD Programs listed some ECDD measures, but did not include processes or guidance as to:

i. which steps to apply in response to the specific ML/TF risks posed by the customer;

ii. how those measures addressed the ML/TF risks posed by customer activity; or

iii. the customer risks that were acceptable and those that were not.

b. Under the Crown Melbourne ECDD Program, the CTRM was primarily responsible for undertaking ECDD. By reason of the matters pleaded at paragraph a, the ECDD measures were at the discretion of the CTRM, subject to the following:

i. With respect to foreign PEPs, the CTRM was required to undertake reasonable measures to establish source of wealth and funds, but these processes were inadequate for the reasons pleaded at paragraph 667, and therefore largely left to discretion.

ii. Senior management approval was required for an ongoing business relationship with foreign PEPs, but the AML Team (not senior management) was authorised to make these decisions in the first instance.

c. Under the Crown Perth Program, the AMLCO (or designee from 2 November 2018) had the discretion to determine the ECDD measures that would be performed, subject to the following.

i. Foreign PEPs were not automatically rated high risk. A range of ECDD measures were required for foreign PEPs, but were not subject to appropriate guidance or criteria, and therefore left largely to the judgment of the AMLCO.

ii. Senior management approval was required for ongoing business relationships and decisions about whether to provide designated services to foreign PEPs. However, there were no processes to consistently refer foreign PEPs to senior management.

d. The staff exercising discretion under the ECDD Program did not receive adequate training.

Particulars

See paragraph 608.

e. The ECDD Programs did not set out appropriate ECDD measures that were aligned to the nature, size and complexity of Crown Melbourne's and Crown Perth's business, and the ML/TF risks posed by customers.

f. In particular, the ECDD Program did not include appropriate procedures to ensure:

i. analysis of the full suite of designated services received by customers across multiple transaction chains and channels, including designated services provided under table 1, s6;

ii. analysis of third party transactions;

iii. that KYC information would be clarified and verified, beyond re-performing standard KYC checks; or

iv. source of wealth or source of funds would be appropriately assessed (see paragraph 667 below).

Particulars

Rule 15.10 of the Rules.

Source of wealth and source of funds

667. From 1 March 2016 to 1 November 2020, the ECDD Programs did not include appropriate systems and controls for Crown Melbourne and Crown Perth to obtain, analyse and record source of wealth and source of funds information with respect to customers for the purposes of carrying out ECDD for the following reasons.

a. See the matters pleaded at paragraph 122.

b. The ECDD Program did not specify what source of wealth or source of funds checks should be conducted for the purposes of ECDD:

i. The Crown Melbourne ECDD Programs stated that reasonable measures would be undertaken to establish source of wealth and source of funds.

ii. The Crown Melbourne ECDD Program stated that enquiries would be made to the appropriate department manager to obtain further information on source of wealth and source of funds.

iii. These processes were inadequate, not subject to any guidance or criteria, and not appropriately risk-based.

c. There were no processes to ensure that source of wealth and source of funds information obtained by VIP International or ICB for the purposes of credit risk assessments were referred, on a risk basis, to the AML/Financial Crime teams for the purposes of ECDD.

d. The ECDD Program did not include or incorporate any guidance or criteria for the analysis of source of wealth and source of funds information, having regard to ML/TF risks or any ML/TF risk appetite to be accepted with respect to customers.

e. Crown Melbourne and Crown Perth sought source of wealth and source of funds information from junket or international VIP customers where it was extending credit, but did not include procedures in its ECDD Program to assess this information from an AML/CTF perspective. Rather, this information was used to assess credit risk only.

f. The Standard Part A Programs did not include appropriate risk-based controls to identify customers whose source of wealth or source of funds was unexplained or possibly illegitimate, and in such cases, to determine whether:

i. specific transactions should be processed; or

ii. an ongoing relationship with the customer was within risk appetite.

g. In the absence of appropriate information and guidance about source of wealth and source of funds, Crown Melbourne and Crown Perth were unable to carry out appropriate risk-based ECDD measures. For example, Crown Melbourne and Crown Perth were not in a position to understand the purpose of customer transactions, or the ML/TF risks they posed. Nor were they in a position to determine the ML/TF risk posed by the customer and the ongoing business relationship.

Particulars

Rules 15.10(1)(c), (2) and (5) of the Rules.

In June 2018, the Chief Legal Officer of Crown Resorts, who was also the AMLCO for both Crown Melbourne and Crown Perth, received a recommendation from the Group General Manager AML that Crown

Melbourne's ECDD processes should be updated to make it clearer as to when source of funds information would be sought and as to what specified source of wealth or source of funds checks would be conducted - particularly with respect to third party transfers.

The Group General Manager also recommended that the issue of source of wealth/funds under the AML/CTF Programs be taken to the Board for its consideration as to its comfort level.

Senior management approval

668. From 1 March 2016 to 1 November 2020, the ECDD Programs did not include appropriate systems and controls to seek senior management approval:

a. for continuing business relationships with customers, having regard to the ML/TF risks reasonably faced;

b. on whether a designated service should be provided to a customer;

c. on whether a transaction or particular transactions should be processed

for the reasons pleaded at paragraphs 669 to 674 below.

Particulars

Rules 15.10(6), (7) and 15.11 of the Rules.

669. As the Crown Melbourne and Crown Perth Boards did not determine the ML/TF risk appetite to be accepted with respect to customers, there was no criteria against which senior management could appropriately determine whether to approve:

a. a continued business relationship with a customer;

b. the provision of a designated service (such as a loan or remittance service) to a customer;

c. a transaction or particular transactions.

Particulars

Rules 15.10(6), (7) and rule 15.11 of the Rules.

With respect to paragraph 669c, see also paragraph 450.

670. The ECDD Programs did not include appropriate processes to escalate high risk customers to senior management to make decisions with respect to the matters pleaded at paragraph 668.

Particulars

By no later than June 2018, the Chief Legal Officer of Crown Resorts, who was also the AMLCO for both Crown Melbourne and Crown Perth, was briefed by the Group General Manager - AML on concerns in relation to the matters pleaded at paragraph 670 with respect to the Crown Melbourne ECDD Program.

671. The **WOL and NRL processes** were engaged on occasion by Crown Melbourne and Crown Perth to refer customers to management or senior management in circumstances where the

customer had come to Crown Melbourne's or Crown Perth's attention as involving higher ML/TF risks:

a. A WOL was a decision by Crown Melbourne to issue a withdrawal of the common law licence for a specific customer to enter the casino premises.

b. An NRL was a decision by Crown Perth to issue a notice revoking the common law licence for a specific customer to enter the casino premises.

c. The purpose of the WOL and NRL processes, as set out in the written policies, was to withdraw the common law licence of customers to enter casino premises where 'non-gaming behavioural issues' emerged.

d. The WOL and NRL processes did not set out criteria to enable Crown Melbourne or Crown Perth to appropriately or consistently consider, having regard to ML/TF risk, whether an ongoing business relationship was appropriate.

e. The issue of a WOL or NRL could be, but was not necessarily, accompanied by a decision to place a 'stop code' on a customer's DAB account to prevent further transactions.

f. As a result, a WOL or NRL did not necessarily prevent the customer from receiving further designated services.

Particulars

Rules 15.10(6), (7) and 15.11 of the Rules.

672. The **POI Committee process** was engaged on occasion by Crown Melbourne and Crown Perth in circumstances where customers had come to Crown Melbourne's or Crown Perth's attention as involving higher ML/TF risks:

a. From 1 March 2016 to 1 November 2020, Crown Melbourne and Crown Perth each had committees that considered customers regarded as 'persons of interest' (**POI**), and that could decide whether or not the customer should be allowed to continue to frequent the Crown Melbourne and Crown Perth casinos, respectively (the POI Committee process).

b. The Crown Melbourne POI Committee met periodically and on an ad hoc basis.

c. The Crown Perth POI sub-committee met fortnightly, although it did not meet formally between mid-August 2020 and March 2021.

d. Between 1 January 2015 and October 2020, any Crown Melbourne or Crown Perth employee could refer a customer or prospective customer to the Crown Melbourne or Crown Perth POI Committee in any circumstance.

e. The POI Committee process did not set out criteria to enable Crown Melbourne or Crown Perth to appropriately or consistently consider, having regard to ML/TF risk, whether an ongoing business relationship was appropriate.

f. The Patron Decision Assessment (**PDA**) tool, which set out criteria for the POI Committee to consider customers presented to them, was not implemented until October 2020.

g. With respect to foreign PEPs:

i. Under the Crown Melbourne ECDD Program, senior management approval was required for an ongoing business relationship with foreign PEPs, but the AML Team (not senior management) was authorised to make this decision in the first instance.

ii. Under the Crown Perth Program, senior management approval was required for ongoing business relationships and decisions about whether to provide designated services to foreign PEPs. However, there were no processes to consistently refer foreign PEPs to senior management.

Particulars

Rules 15.10(6), (7) and 15.11 of the Rules.

673. The processes for senior management to approve loans and credit limits (items 6 and 7, table 1, s6 designated services) had regard to credit risk, not ML/TF risk.

674. To the extent that senior management within the VIP International or Credit Control teams considered whether to provide designated services to a customer (such as a loan) or whether to continue an ongoing business relationship, decisions were made from the perspective of credit risk, not ML/TF risk.

Information management and records

675. From 1 March 2016 to 1 November 2020, the ECDD Programs were not supported by appropriate information management and record keeping.

676. By reason of the deficiencies in information management and record keeping pleaded at paragraphs 613 to 626:

a. Crown Melbourne and Crown Perth did not have a full view of customers' transactions for ECDD purposes; and

b. the procedures in the ECDD Program were not capable by design of operating as intended.

677. From November 2016, if Crown Melbourne or Crown Perth collected KYC information on a customer, it was intended to be stored in LUI/CC2.

678. Whilst LUI was introduced to Crown Perth and Crown Melbourne in November 2016:

a. It was not used to register customers at Crown Melbourne and Crown Perth until October 2019.

b. The Standard Part A Programs did not include appropriate processes to ensure customer information was consistently entered on to LUI/CC2.

c. At all times, data entered into LUI and CC2 needed to be synchronised with SYCO records in order for customer transactions to be linked to up to date customer profiles.

d. Whilst KYC information in relation to a customer collected in one property could be accessed and relied upon by the other property when dealing with that customer, there were no processes in place for this to occur.

Particulars

See Customer 26.

e. Consolidation of customer data was not completed until 2019 for all customers. Before that time, KYC information from Crown Melbourne for VIP customers would not have been available to Crown Perth and vice versa.

f. The Standard Part A Programs did not include any processes to facilitate use of LUI for ECDD purposes.

679. Prior to May 2021, there were no policies or procedures requiring the Crown Melbourne AML/Financial Crime teams to have regard to information in SEER and, as a result, information on SEER was reviewed on an ad hoc basis only.

680. Crown Melbourne and Crown Perth created and maintained customer records and accounts using multiple customer PIDs and multiple names.

a. From November 2019, Crown Melbourne and Crown Perth instituted a policy requiring new customers who opened an account to obtain a single PID number which is to be held for that customer across all Crown venues.

b. Prior to November 2019, Crown Melbourne and Crown Perth could issue more than one PID to the same customer:

i. Customers were issued with different PIDs each time they played on a different program, as SYCO was not able to apply different programs of play to the same PID.

ii. Customers could open multiple DAB accounts and safekeeping accounts with different PIDs.

iii. Some junket operators operated multiple junkets with multiple PIDs.

c. Prior to November 2019, the same PID could be issued by Crown Melbourne to one customer and by Crown Perth to a different customer.

d. Crown Melbourne and Crown Perth did not have appropriate systems and controls in place to ensure that customers were not issued with accounts and PIDs in different names.

e. Further, Crown Melbourne and Crown Perth had a practice of creating ‘pseudonym PIDs’ for certain customers.

Particulars

The practice of creating pseudonym PIDs appears to have developed a number of years ago to accommodate concerns held by a relatively small number of VIP customers.

Such customers were often concerned that casino floor staff and/or other customers may identify them and use their rated play activity to their advantage (and the high profile customer's detriment), either by providing the high profile customer's gaming data to rival casinos (in the case of Crown staff), or by learning personal information about the high profile customer (in the case of other customers).

To address such customers' concerns, a pseudonym PID could be created, which the customer could then use for the recording of gaming and other activity at the casino, such as accrual of complimentaries. A name other than the name (or names) by which

the customer was known (a pseudonym) was assigned to the customer in the pseudonym PID.

The pseudonym PID was linked to a primary PID in the customer's real name. Staff with a certain level of security level clearance (including Cage management, certain VIP international management, legal and compliance staff (including AML staff) and surveillance management staff) were able to view both the pseudonym PID and the primary PID in SYCO.

The scope and implications of the use of pseudonym PIDs are still under investigation by Crown Melbourne and Crown Perth.

f. The process of remediating customer data to ensure each customer has a single unique PID and a single account is still ongoing.

Particulars

By no later than June 2018, the Chief Legal Officer of Crown Resorts, who was also the AMLCO for both Crown Melbourne and Crown Perth was briefed by the Group General Manager AML (Melbourne) on an 'IT issue' relating to the existence of multiple accounts for customers which was adding to the workload of the CTRM and the Legal Officer - AML in Perth and impacting transaction monitoring. The Chief Legal Officer/AMLCO was advised that this IT issue was complicating disclosures to law enforcement agencies and required multiple data points to be checked to ensure that information on SMRs was correct.

681. At no time did Crown Melbourne or Crown Perth consistently keep records of risk information it obtained for the purposes of ECDD; nor were ECDD records kept in a central repository.

682. To the extent records were made of customer risk assessments, ECDD or credit risk assessments, they were stored on local drives and shared via email. Crown Perth also retained some ECDD records on CURA or within hard copy files.

683. For the reasons set out at paragraphs 657 to 664, Crown Melbourne's and Crown Perth's IT and record keeping systems were not capable by design of providing a complete or accurate view of customers' transactions and ML/TF risk profiles for ECDD purposes.

The Standard Part A Programs - Appropriate systems and controls to ensure SMR, TTR and IFTI reporting

684. At all times, Part A of an AML/CTF program was required to include systems and controls designed to ensure compliance with the obligation to report:

a. suspicious matter reports, or **SMRs**, under s41 of the Act;

b. threshold transaction reports, or **TTRs**, under s43 of the Act;

c. international funds transfer instructions, or **IFTIs**, under s45 of the Act.

Particulars

Rule 8.9.1(2) of the Rules, made for the purposes of section 84(2)(c) of the Act.

SMR reporting

685. From 1 March 2016 to 1 November 2020, the Standard Part A Programs did not include appropriate systems and controls designed to ensure compliance with the obligation to report SMRs under s 41 of the Act.

a. The policies and guidance relating to suspicious matter reporting were inadequate and did not cover all ML/TF risks reasonably faced or all designated services.

b. The deficiencies in the transaction monitoring programs, as pleaded at paragraphs 586 to 651, meant that Crown Melbourne and Crown Perth were unable to consistently identify suspicious activity within the meaning of s41 of the Act, having regard to unusual patterns of transactions, which had no apparent economic or visible lawful purpose.

Particulars

Rules 15.4 to 15.8 of the Rules.

c. Escalation processes for unusual or suspicious activity were inadequate:

i. Workflows were manual and relied on frontline staff on the casino floor or the Cage raising 'internal SMRs' or UARs to the Financial Crime team.

ii. Frontline staff did not receive adequate AML/CTF risk awareness training.

Particulars

See paragraph 608.

iii. The internal SMR form did not cover all designated services or ML/TF typologies.

d. Resourcing of the systems and controls for SMR reporting were inadequate, and were therefore incapable by design of operating as intended.

Particulars

Prior to July 2018, the CTRM, alone, was responsible for reviewing all internal SMRs to determine whether a report to AUSTRAC under s41 was required.

From July 2018 this review was performed by the Financial Crime team. From July 2018 to November 2020, the Financial Crime team (comprised of 5 persons as at January 2020) had this responsibility.

By no later than June 2018, the Chief Legal Officer of Crown Resorts, who was also the AMLCO for both Crown Melbourne and Crown Perth, was advised by the Group General Manager AML that the CTRM (Melbourne) essentially acted as a post box on UAR forms submitted by frontline staff, supplementing them where relevant but otherwise just passing them on, and was advised that resourcing in the AML team in both Melbourne and Perth was stretched to the limit.

Until 24 September 2020, at Crown Perth, persons occupying the AML Officer and Legal Officer – AML roles were responsible for reviewing the internal SMR forms and determining whether the SMR was to be filed with AUSTRAC.

e. Dispersed data sources for customer information limited Crown Melbourne's and Crown Perth's ability to understand a customer's transactional activity and to determine whether any particular activity was unusual.

Particulars

See paragraph 683.

f. Dispersed data sources, multiple customer IDs and multiple accounts also impacted on Crown Melbourne's and Crown Perth's ability to include accurate customer information in SMRs (for example, as to win/loss/turnover on an aggregate basis).

g. Prior to November 2017, the CTRM in Melbourne was not receiving surveillance and security reports.

h. Credit Control (VIP International, Crown Resorts) who were responsible for identifying IFTIs for reporting for Crown Melbourne, were not given appropriate AML/CTF training to enable them to identify potential suspicious activity relating to international transfers.

i. SMRs relating to suspicious activity on junket programs were likely to be reported under the junket operator's name (with the junket representative as agent) rather than under the name of the junket player who conducted the transaction.

j. This made it difficult for AUSTRAC and its law enforcement partners to understand the role of different parties to the suspicious activity, including what transactions took place, the source of the funds, who instructed the movement of funds, the recipient of the funds and further details of the transaction.

k. There were no assurance processes regarding SMR obligations.

l. There was inadequate documentation for and monitoring over the SMR reporting process.

686. On or about September 2020, Crown Melbourne and Crown Perth commenced a number of transaction monitoring lookbacks over designated services provided to customers from 1994.

687. As a result of these transaction monitoring lookbacks and other customer-related lookback reviews, Crown Melbourne and Crown Perth have formed suspicions resulting in over 400 SMRs being given to the AUSTRAC CEO to date.

TTR reporting

688. From 1 March 2016 to 1 November 2020, the Standard Part A Programs did not include appropriate systems and controls designed to ensure compliance with the obligation to report TTRs under s43 of the Act.

a. The policies and guidance relating to TTR reporting were inadequate and did not apply to all designated services.

b. The processes for TTR reporting were manual, prone to human error and not subject to appropriate assurance.

Particulars

For example, prior to October 2020, uncarded transactions of $10,000 or more at tables were not recorded in SYCO against KYC information or a PID. TTR reporting was reliant upon a manual

issues/incident log. This manual process was subject to human error and could not be the subject of appropriate assurance.

c. Crown Melbourne did not make and keep complete records of all designated services involving cash, and therefore did not have appropriate systems in place to identify and report all TTRs.

Particulars

For example, prior to April 2018, Suncity staff members would dispense Crown gaming chips in exchange for cash to junket players. In addition, junket players could exchange Crown chips for cash at the Suncity cash administration desk.

Crown Melbourne made no record of cash transactions conducted in the private gaming rooms made available to the Suncity junket, including through the Suncity cash administration desk.

d. TTRs relating to transactions conducted through junket programs were likely to be reported under the junket operator's name (with the junket representative as agent) rather than under the name of the junket player who conducted the transaction.

e. This made it difficult for AUSTRAC and its law enforcement partners to understand the role of different parties to the threshold transaction, including what transactions took place, the source of the funds, who instructed the movement of funds, the recipient of the funds and further details of the transaction.

f. In relation to EGMs and ETGs at Crown Melbourne:

i. A customer could insert up to $9,899 (the note acceptor limit) into an EGM or ETG.

ii. The customer could then insert coins, taking the amount inserted above the $10,000 threshold.

iii. The customer could either play or hit collect to obtain a TITO ticket.

iv. Crown Melbourne did not carry out the ACIP or file a TTR in this scenario.

Particulars

By no later than June 2018, the Chief Legal Officer of Crown Resorts, who was also the AMLCO for both Crown Melbourne and Crown Perth, was briefed by the Group General Manager AML on the matters pleaded at f.

g. There was inadequate documentation for and monitoring over the TTR reporting process.

IFTI reporting

689. From 1 March 2016 to 1 November 2020, the Standard Part A Programs did not include appropriate systems and controls designed to ensure compliance with the obligation to report IFTIs under s45 of the Act.

a. Processes at Crown Melbourne were manual and not subject to appropriate assurance.

b. IFTIs relating to junket programs were likely to be reported under the junket operator's name (with the junket representative as agent) rather than under the name of the junket player who conducted the transaction.

c. This made it difficult for AUSTRAC and its law enforcement partners to understand the role of different parties to the IFTI, including what transactions took place, the source of the funds, who instructed the movement of funds, the recipient of the funds and further details of the transaction.

d. At Crown Melbourne, there was no central oversight of IFTI reporting by the CTRM or Financial Crime team.

Particulars

By no later than June 2018, the Chief Legal Officer of Crown Resorts, who was also the AMLCO for both Crown Melbourne and Crown Perth, was briefed by the Group General Manager - AML on the lack of oversight by the AML/Financial Crime team with respect to IFTI reporting at Crown Melbourne.

Recommendations to the Chief Legal Officer/AMLCO to bring IFTI reporting under the oversight of the AML/Financial Crime team were not adopted due to lack of resources in that team.

690. By reason of the matters pleaded in paragraphs 684 to 689, the Standard Part A Programs did not comply with rule 8.9.1(2) of the Rules from 1 March 2016 to 1 November 2020.

691. By reason of the matters pleaded in paragraph 690, the Standard Part A Programs did not comply with s 84(2)(c) of the Act from 1 March 2016 to 1 November 2020.

The Standard Part B Programs – the applicable customer identification procedures

692. From 1 March 2016 to 1 November 2020, Crown Melbourne's and Crown Perth's Standard AML/CTF Program included a Part B Program (the **Standard Part B Programs**).

a. Crown Melbourne's Standard Part B Program was set out in clause 20 and Annexure I.

b. Crown Perth's Standard Part B Program was set out in clauses 18 to 20 and Annexures F and G.

Particulars

Chapters 4 and 10 and rule 14.4 of the Rules.

693. From 1 March 2016 to 1 November 2020, the Standard Part B Programs were not:

a. programs the sole or primary purpose of which was to set out the applicable customer identification procedures (**ACIPs**) for the purposes of the application of the Act to customers of the reporting entity; and

b. that complied with the requirements of the Rules.

Particulars

Section 84(3)(a) and (b) of the Act and Chapter 4 of the Rules.

Also see Chapter 10 and rule 14.4 of the Rules, made under s39 of the Act, which provide for certain exceptions to the application of Part

2 with respect to some designated services provided by Crown Melbourne and Crown Perth.

Also see rule 8.1.6 of the Rules.

694. From 1 March 2016 to 1 November 2020, the Standard Part B Programs did not include appropriate risk-based systems and controls that were designed to enable Crown Melbourne and Crown Perth to be reasonably satisfied, where the customer was an individual, that the customer was the individual he or she claimed to be, for the reasons pleaded at paragraphs 695 to 706.

Particulars

Rule 4.2.2 of the Rules.

695. At no time did the Standard Part B Programs include any risk-based systems and controls to identify customers who were not low risk at the time the ACIP was being carried out:

a. Customers were considered low risk by default.

b. Procedures to trigger a review of this default risk rating were not included in Standard Part B and Programs and were unlikely to be consistently identified at the time ACIP was being conducted.

c. The Standard Part B Programs were accordingly not risk-based.

Particulars

Clause 13 of the Standard Part A Programs.

Rules 4.2.2 and 4.1.3 of the Rules.

696. At no time did the Standard Part B procedures consider the ML/TF risk posed by customer types.

a. Junket operators, junket representatives and junket players should not have been considered low risk by default for the purposes of ACIP.

b. International premium program players should not have been considered low risk by default for the purposes of ACIP.

c. PEPs, including foreign PEPs, should not have been considered low risk by default for the purposes of ACIP.

Particulars

Clause 13 of the Standard Part A Programs.

Rules 4.2.2, 4.1.3(1), 4.1.3(2) and 4.13.3 of the Rules.

697. At no time did the Standard Part B Programs consider the ML/TF risk posed by a customer's sources of wealth and funds.

a. Procedures incorporated into the Standard Part B Programs stated a customer's occupation would be requested on all Crown Melbourne and Crown Perth application forms, but completion by the customer was optional.

b. No other risk-based inquiries were made as to source of wealth or funds as part of the ACIP.

Particulars

Rules 4.2.2 and 4.1.3(2) of the Rules.

The complexity and volume of designated services provided to customers, combined with the absence of source of funds and source of wealth information, significantly limited Crown Melbourne's and Crown Perth's ability to fully understand who they were dealing with as a customer.

The failure to obtain appropriate source of wealth/funds information at the time of the ACIP, on a risk-basis, affected the operation of processes in the Standard Part A Programs. For example, this failure impacted Crown Melbourne's and Crown Perth's ability to identify unusual or suspicious transactions, such as unusually high turnover or losses.

698. At no time did the Standard Part B Programs consider the ML/TF risk posed by the nature and purpose of Crown Melbourne's and Crown Perth's business relationships with their customers, including as appropriate, the collection of information relevant to that consideration.

a. In particular, the Standard Part B Programs did not appropriately consider the nature and purpose of the business relationship with customers who were junket operators, junket representatives and junket players.

Particulars

Rules 4.2.2 and 4.1.3(3) of the Rules.

699. At no time did the Standard Part B Programs consider the ML/TF risk posed by the types of designated services Crown Melbourne and Crown Perth provided, together with the methods or channels by which designated services were delivered.

a. The Standard Part B Programs did not consider the ML/TF risks of designated services provided under table 1, s6 (such as items 6 and 7, table 1, s6 loans and overseas/domestic remittance services under items 31 and 32, table 1, s6).

b. The Standard Part B Programs did not consider the ML/TF risks involved in providing table 1, s6 designated services (remittance services) and item 13, table 3, s6 (DAB accounts) designated services through non-face-to-face channels, including through the Crown Patron account channels.

c. The Standard Part B Programs did not consider the ML/TF risks of providing table 1 and table 3, s6 designated services to customers through junket channels.

Particulars

Rules 4.2.2, 4.1.3(5) and (6) of the Rules.

700. At no time did the Standard Part B Programs consider the ML/TF risk posed by the foreign jurisdictions with which Crown Melbourne and Crown Perth dealt.

a. There were no risk-based processes to identify customers from higher risk jurisdictions at the time Crown Melbourne and Crown Perth was conducting the ACIP.

b. Whilst Crown Melbourne asserted it conducted periodic sweeps of the SYCO database for customers with identification from a 'high risk' jurisdiction, which would trigger an

increase to the customer risk rating, this was done on an ad-hoc basis and not as part of the ACIP.

c. Whilst Crown Perth asserted it conducted monthly reviews of jurisdiction risks presented by its customers, this was done on an ad-hoc-basis and not as part of the ACIP.

Particulars

Rules 4.2.2 and 4.1.3(7) of the Rules.

701. At no time did the Standard Part B Programs include appropriate risk-based systems and controls for Crown Melbourne and Crown Perth to determine whether additional KYC information would be collected about a customer and/or verified.

a. Limited procedures to collect or verify additional KYC information about a customer were included in the Standard Part A Programs, but not included in Part B as part of the ACIP and were not triggered at the time ACIP was conducted.

b. The Standard Part B Programs were accordingly not risk-based.

c. The Standard Part B Programs applied the same 'safe-harbour' ACIP to all customers, regardless of risk.

d. There were no risk-based procedures in the Standard Part B Programs to determine whether to collect or verify additional KYC information relating to the beneficial ownership of funds used by the customer with respect to designated services or the beneficiaries of transactions being facilitated by the reporting entity on behalf of the customer including the destination of funds.

Particulars

Rules 4.2.2, 4.2.5 and 4.2.8 of the Rules; and the definition of KYC information in rule 1.2.1 of the Rules.

702. At no time did the Standard Part B Programs include ACIPs to be applied to all customers who Crown Melbourne and Crown Perth were required to identify for the purposes of Part 2 of the Act.

a. There were no procedures in the Standard Part B Programs to determine whether the exemptions in rules 10.1.3 and 10.1.4 did not apply to a customer or prospective customer by reason of rule 10.1.5.

b. Crown Melbourne did not carry out the ACIP with respect to a customer who:

i. inserted up to $9,899 (the note acceptor limit) into an EGM or ETG; and then

ii. inserted coins or a TITO ticket, taking the amount inserted above the $10,000 threshold; and then

iii. either played or hit collect to obtain a TITO ticket.

c. Crown Melbourne gave front line staff discretion as to whether or not to accept ID for a cheque issuance of $10,000 or more.

d. There were no procedures in the Standard Part B Programs that required identification of customers who exchanged foreign currency by way of foreign drafts or travellers' cheques below $1,000 – noting that the exemption in rule 14.4(2)(b) applies to physical currency only.

e. There were no procedures in the Standard Part B Programs to determine whether the exemption in rule 14.4(b) did not apply to a customer or prospective customer.

Particulars

Rule 14.5 of the Rules.

f. There were no risk-based procedures in the Standard Part B Programs to apply ACIPs to prospective customers who were receiving items 6, 7, 31 or 32, table 1, s6 designated services.

Particulars

Section 84(3)(a) of the Act.

See also sections 32 and 39 of the Act; and Part 10 and rule 14.4 of the Rules.

By no later than June 2018, the Chief Legal Officer of Crown Resorts, who was also the AMLCO for both Crown Melbourne and Crown Perth, was briefed by the Group General Manager - AML on the deficiencies pleaded at b and c.

703. At no time did the Standard Part B Programs include appropriate procedures to collect information and documents about an agent of a customer (who was an individual) or to determine whether to verify (and to what extent) the identity of the agent.

a. In particular, the Standard Part B Programs did not contain appropriate ACIPs for identifying junket operators or junket representatives acting as agents for junket players.

b. Crown Melbourne and Crown Perth accepted instructions from junket operators or junket representatives for the transfer of funds on behalf of junket players.

Particulars

Item 31, table 1, s6 of the Act.

c. Crown Melbourne and Crown Perth did not have appropriate systems and controls in place to recognise when a transfer of funds was being carried out by junket operators or junket representatives on behalf of another customer.

d. In the absence of these systems and controls, Crown Melbourne and Crown Perth were unable to identify when the information required by Part 4.11 of the Rules was required to be collected and verified.

Particulars

Part 4.11 of the Rules.

See also paragraph 492.

704. At no time did the Standard Part B Programs include appropriate risk-management systems that would enable Crown Melbourne and Crown Perth to consistently determine whether a customer was a PEP, either before the provision of a designated service to the customer or as soon as practicable after the designated service has been provided:

a. The Standard Part A Programs indicated that PEPs may be identified by screening. As pleaded at paragraph 120, the processes in the Standard Part A Programs for screening for PEPs were inadequate.

Particulars

Rule 4.13.1 of the Rules.

705. At no time did the Standard Part B Programs include appropriate risk-management systems for Crown Melbourne and Crown Perth to:

a. comply with identification requirements in rules 4.2.3 to 4.2.9 of the Rules in respect of a customer who was:

i. a domestic PEP or international organisation PEP who had been assessed as posing a high ML/TF risk; or

ii. a foreign PEP.

b. obtain senior management approval before establishing or continuing a business relationship with the customer;

c. take reasonable measures to establish the customer's source of wealth and source of funds; and

d. comply with Chapter 15 of the Rules, including rule 15.11 with respect to a foreign PEP.

Particulars

Rules 4.13.2 and 4.13.3 of the Rules.

By no later than June 2018, the Chief Legal Officer of Crown Resorts, who was also the AMLCO for both Crown Melbourne and Crown Perth, was advised by the Group General Manager AML that source of funds checks were not being conducted on foreign PEPs, contrary to requirements of rule 4.13.

706. From 1 March 2016 to 1 November 2020, Crown Melbourne's and Crown Perth's information management systems did not enable them to be reasonably satisfied, where the customer was an individual, that the customer was the individual he or she claimed to be.

Particulars

See paragraph 680.

The deficiencies in Crown Melbourne's and Crown Perth's information management limited their ability to know who their customers were, as at the time the ACIP was carried out.

Rules 4.2.2 and 15.3 of the Rules.

A review of Crown Melbourne's and Crown Perth's records conducted in 2021 by an external auditor identified 2,195 customers who shared two or more KYC identifiers (address, identification number, passport number, telephone number) with another customer with a different PID. Of the 2,195 customers identified, 83 customers were also identified as part of the external auditor's review for other typologies.

707. By reason of the matters pleaded in paragraphs 693 to 706, the Standard Part B Programs did not:

a. set out the ACIPs for the purposes of the application of the Act to all customers of Crown Melbourne and Crown Perth; and

b. comply with Chapter 4 of the Rules from 1 March 2016 to 1 November 2020.

708. By reason of the matters pleaded in paragraph 707, the Standard Part B Programs did not comply with s 84(3)(a) and (b) of the Act from 1 March 2016 to 1 November 2020.

The Joint AML/CTF Program – Crown Melbourne and Crown Perth

The Joint Part A Program

709. On and from 2 November 2020, Crown Melbourne and Crown Perth each purported to adopt and maintain a Joint Part A Program: see paragraph 52.

710. On 21 December 2021, the Crown Resorts Board approved a revised Joint Part A Program, which was expressed to be effective from 31 January 2022.

The FCCCP

711. The Financial Crime & Compliance Change Program (**FCCCP**) was approved by the Crown Resorts Board on 24 May 2021.

712. The FCCCP is a roadmap for significant development and change in Crown Melbourne's and Crown Perth's financial crime and compliance program.

713. The FCCCP aims to raise the maturity of the financial crime and compliance regime to 'advanced' by December 2022.

714. As part of the FCCCP, the 'Crown DBG ML/TF Enterprise Wide Risk Assessment' (**ML/TF EWRA**) was completed in December 2021 following endorsement from the ML/TF Design Authority. The assessment period for the ML/TF EWRA was July 2020 to 30 June 2021.

715. The results of the ML/TF EWRA were presented to the Crown Resorts Board on 21 December 2021. The results of the ML/TF EWRA informed the updates to the Joint Part A Program approved on 21 December 2021.

716. The ML/TF EWRA assessed the inherent and residual ML/TF risk for the Crown Melbourne and Crown Perth DBG as high (**the DBG**).

717. The Joint Part A Program controls for the DBG were assessed and rated as 'not assessed', which is equivalent to an unsatisfactory controls rating.

718. The Joint Part A Program controls were not assessed for the purposes of the ML/TF EWRA because the controls are not yet comprehensively designed and operating effectively. Testing on the operating effectiveness of controls is expected to commence soon.

719. An independent review of the Joint Part A Program has commenced and is due to be completed soon.

720. The ML/TF EWRA report contains a number of recommendations, including that the DBG:

a. conduct a re-assessment of what designated services it provides. This is expected to be complete by 31 June 2022.

b. conduct a further ML/TF EWRA within 12 months of the date of endorsement of the 'baseline EWRA', taking into account the significant uplift activities in-flight. This is expected to commence in the second half of 2022.

c. review and update the ML/TF methodology for all future ML/TF EWRAs. This is expected to commence in the second half of 2022.

d. scope further uplifts for ECDD.

e. give further consideration to the impact of the ML/TF risks of DAB accounts and safekeeping accounts on customer risk profiles.

f. perform a completeness/gap assessment to take into account both those controls which may exist but have not been formally documented, and those controls still in development. This is scheduled to be complete by the end of 2022.

g. document ML/TF controls in a digital and centralised control library and allocated to specific business units. This is scheduled to be complete by the end of 2022.

h. consider establishing an ML/TF issues and events register to record, monitor and remediate potential and realised ML/TF concerns. This is scheduled to be complete by the end of 2022.

i. continue training and awareness sessions with respect to ML/TF risks, and the vulnerabilities inherent in products and services.

721. The ML/TF EWRA identified notable ML/TF controls that are still in the process of being designed and uplifted, including:

a. Customer risk data attributes' enhancement mandating the capture of member occupation, place of birth and citizenship for all new customers at onboarding.

b. Automated TM alert enhancements are being designed to support predictive customer behavioural analysis expected to improve future risk assessment data reference points and processes.

c. Data infrastructure uplift.

d. ECDD framework and process uplift are in development.

e. Enhanced ML/TF focused controls for peer-to-peer poker are in development.

722. However, as the recommended remediation and uplift of controls is still in progress, the Joint Part A Program is not yet aligned to the ML/TF risks reasonably faced by Crown Melbourne and Crown Perth with respect to the provision of designated services.

723. As a result of the matters pleaded at paragraphs 711 to 722, the Joint Part A Program does not yet have the primary purpose of identifying, mitigating and managing ML/TF risks reasonably faced by Crown Melbourne and Crown Perth with respect to the provision of designated services and does not yet comply with the requirements of the Rules.

Particulars

Sections 85(2)(a) and (c) of the Act and rules 9.1.3. 9.1.4, 9.1.5, and rules 15.2 to 15.11 of the Rules.

724. By reason of the matters pleaded in paragraph 723, the Joint Part A Program did not comply with s 85(2)(a) and (c) of the Act from 2 November 2020.

The Joint Part B Program

725. On and from 2 November 2020, Crown Melbourne and Crown Perth each purported to adopt and maintain a Joint Part B Program.

Particulars

See paragraph 53.

726. Pending a further enterprise-wide risk assessment, Crown Melbourne and Crown Perth are not yet in a position to include appropriate risk-based ACIPs in its Joint Part B Program that

are designed to enable Crown Melbourne and Crown Perth to be reasonably satisfied, where a customer is an individual, that the customer is the individual he or she claimed to be.

a. The Joint Part B Program is yet to include appropriate risk-based systems and controls to identify customers who are not low risk at the time the ACIP is being carried out.

b. The Joint Part B Program is yet to include appropriate risk-based systems and controls for Crown Melbourne and Crown Perth to determine whether and when additional KYC information should be collected about a customer and/or verified.

c. The Joint Part B Program continues to apply the same 'safe-harbour' ACIP to all customers, regardless of risk.

d. The Joint Part B Program does not yet include appropriate ACIPs to be applied to all customers who Crown Melbourne and Crown Perth are required to identify for the purposes of Part 2 of the Act.

Particulars

Rules 9.1.6 and 4.2.2 of the Rules.

Section 84(3)(a) of the Act.

See also sections 32 and 39 of the Act; and Part 10 and rule 14.4 of the Rules.

See paragraphs 692 to 706 above.

727. For the reasons pleaded at paragraph 726, on and from 2 November 2020, the Joint Part B Program was not an AML/CTF Program the sole or primary purpose of which was to set out the ACIPs for the purposes of the application of the Act to customers of the reporting entities and that complied with the requirements of the Rules.

728. By reason of the matters pleaded in paragraph 727, the Joint Part B Program did not comply with s 85(3)(a) and (b) of the Act from 2 November 2020.

ONGOING CUSTOMER DUE DILIGENCE – SECTION 36 OF THE ACT

729. At all times from 1 March 2016, Crown Melbourne was required by s36(1) of the Act to:

a. monitor its customers in relation to the provision by Crown Melbourne of designated services at or through a permanent establishment of Crown Melbourne in Australia, with a view to identifying, mitigating and managing the risk that Crown Melbourne may reasonably face that the provision of a designated service at or through a permanent establishment of Crown Melbourne in Australia might (whether inadvertently or otherwise) involve or facilitate money laundering; and

b. do so in accordance with the Rules.

730. At all times from 1 March 2016, Crown Melbourne was required by the Rules made under s36(1), among other things:

a. to have regard to the nature, size and complexity of its business and the type of ML/TF risk it might reasonably face, including the risk posed by customer types;

b. to include a transaction monitoring program in its Part A program that, among other things:

i. includes appropriate risk-based systems and controls to monitor the transactions of customers;

ii. has the purpose of identifying, having regard to ML/TF risk (as defined in the Rules), any transaction that appears to be suspicious within the terms of s 41 of the Act;

iii. has regard to unusual patterns of transactions, which have no apparent economic or visible lawful purpose;

c. to include an enhanced customer due diligence program in its Part A program that complies with the requirements of the Rules; and

d. to apply the enhanced customer due diligence program when:

i. Crown Melbourne determines under its risk-based systems and controls that the ML/TF risk (as defined in the Rules) is high;

ii. a designated service is being provided to a customer who is or who has a beneficial owner who is, a foreign PEP; or

iii. a suspicion has arisen for the purposes of s41 of the Act.

e. to undertake the measures specified in rules 15.10(2) and 15.10(6) in the case of a customer who is a foreign PEP.

Particulars

Section 36(1) of the Act and rules 8.1.3, 8.1.4 and 15.4 to 15.11 of the Rules.

Paragraphs 584 and 652 of the pleadings.

JUNKET OPERATORS

Customer 1

731. Customer 1 was a customer of Crown Melbourne from 1 April 2010 to 22 January 2021.

732. From at least 1 April 2010, Crown Melbourne provided Customer 1 with designated services within the meaning of table 1 and table 3, s6 of the Act.

733. From at least 1 April 2010 to 25 February 2020, Customer 1 received designated services within the meaning of table 1 and table 3, s6 of the Act as a junket operator at Crown Melbourne.

Particulars to paragraphs 732 and 733

On 4 September 2009, Crown Melbourne entered into a NONEGPRA with Customer 1 to operate junkets at Crown Melbourne. Between 1 March 2016 and 1 March 2020, Customer 1 operated at least 115 junket programs at Crown Melbourne, including 49 programs under an initial PID, 50 programs under a second PID, 9 programs under a third PID and 7 programs under a fourth PID. During this period, Customer 1 had approximately 70 junket representatives.

On 1 April 2010, Crown Melbourne opened a credit facility for Customer 1 under an initial PID. On 14 September 2020, Crown Melbourne closed Customer 1's credit facility.

Crown Melbourne opened a DAB account and safekeeping account for Customer 1 on the following occasions:

- 23 June 2010 under an initial PID;
- 10 August 2011 under a second PID;
- 6 February 2014 under a third PID;
- 6 February 2014 under a fourth PID;
- 26 November 2019 under a fifth PID; and
- 21 December 2020 under a sixth PID.

On 22 January 2021, the WOL took effect at Crown Melbourne.

734. Customer 1 was a customer of Crown Perth from 8 June 2011 to 29 January 2021.

735. From at least 8 June 2011, Crown Perth provided Customer 1 with designated services within the meaning of table 1 and table 3, s6 of the Act.

736. From at least 8 June 2011 to 25 February 2020, Customer 1 received designated services within the meaning of table 1 and table 3, s6 of the Act as a junket operator and as a junket player at Crown Perth.

Particulars to paragraphs 735 and 736

On 29 June 2010, Crown Perth entered into a NONEGPRA with Customer 1 to operate junkets at Crown Perth. Between 27 June 2016 and 25 March 2020, Customer 1 operated at least 76 junket programs at Crown Perth, including 48 under an initial PID, one under

a second PID, 22 under a third PID and five under a fifth PID. During this period, Customer 1 had approximately 70 junket representatives.

On 1 April 2010, Crown Perth opened a FAF for Customer 1 under an initial PID.

Crown Perth opened a DAB account and safekeeping account for Customer 1 on the following occasions:

- 29 June 2010 under an initial PID;
- 5 February 2014 under a second PID;
- 5 February 2014 under a third PID;
- 24 January 2015 under a fourth PID;
- 20 February 2015 under a fifth PID; and
- 16 September 2019 under a sixth PID.

On 29 January 2021, an NRL took effect at Crown Perth with respect to Customer 1.

The ML/TF risks posed by Customer 1

737. By 1 March 2016, higher ML/TF risks were indicated by the nature and purpose of Customer 1's business relationship with Crown Melbourne and Crown Perth, the nature of the transactions he had been conducting, together with the suspicions Crown Melbourne itself had formed with respect to Customer 1.

Particulars

Section 36(1)(a), (b) of the Act and Chapter 15 of the Rules.

Customer 1 was a junket operator and junket player. He received designated services through the channel of junket programs. This channel lacked transparency: see paragraph 477.

Junket programs – Crown Melbourne

By around March 2016, Customer 1 had operated approximately 91 junket programs at Crown Melbourne. Crown Melbourne recorded that the total turnover for those programs was $8,392,495,297, with losses of $105,180,811. Commissions of $64,952,805 were payable by Crown Melbourne to Customer 1.

Junket programs – Crown Perth

By around 1 March 2016, Customer 1 had operated approximately 40 junket programs at Crown Perth. Crown Perth recorded that the total turnover for those programs was $743,842,494, with losses of $8,066,976. Commissions of $3,813,012 were payable by Crown Perth to Customer 1.

Credit facilities

By 1 March 2016, Crown management had approved numerous credit facilities for Customer 1's junkets prior to the junket programs

in various amounts, up to AUD$30,000,000 and HKD225,000,000. From mid-2013, Crown management approved a standing credit line with a limit of $5,000,000, which would be reviewed by Crown management on a monthly basis. This limit was increased to $30,000,000 from approximately February 2014.

SMRs

Between 2010 and February 2016, Crown Melbourne gave 99 SMRs to the AUSTRAC CEO with respect to Customer 1, which reported:

- 79 SMRs related to patterns of suspicions relating to key player losses and unusual activity by a junket representative of Customer 1's junket;
- transactions with unrelated third parties;
- a series of three enquiries by patrons concerning the possibility of depositing a large sum of cash (approximately $3,000,000 to $3,500,000) to the account of the Suncity junket, in circumstances where Crown was not aware if the conversations were linked, but was aware that three conversations about similar amounts occurred within a short period of time; and
- the transfer of a large amount of funds between the DAB account of a key player of both the Suncity junket and Customer 10's junket, and both junkets' DAB accounts.

Collectively, the SMRs given to the AUSTRAC CEO between 30 June 2010 and 1 February 2016 reported total wins of AUD$22,379,000 and HKD13,771,600, as well as total losses of AUD$138,391,263 and HKD70,364,575.

Other red flags

From March 2012, media articles available from open source searches referred to Customer 1, reported that his associates were allegedly linked to organised crime, and also referred to Customer 1 as a member of a foreign political advisory body.

In addition to the transactions reported above, in 2012 and 2013, Customer 1 sought to repay credit extended to him by Crown Melbourne by making payments from one of his companies (A$748,043 on 6 June 2012; HKD3,934,658.18 on 25 February 2013). These transactions were reversed at Crown Melbourne's request.

On 15 May 2014, an enquiry was made by law enforcement in relation to Customer 1.

Between 11 July 2014 and 1 March 2015, Customer 1 engaged in transactions indicative of ML/TF typologies involving quick turnover of funds (without betting) on three occasions:

- on 11 July 2014, $672,801 was deposited into Customer 1's DAB account by telegraphic transfer, then $672,801 was withdrawn from his DAB account by telegraphic transfer on the same day;
- on 29 January 2015, $30,000 was deposited into Customer 1's DAB account by telegraphic transfer, then $30,000 was withdrawn in cash from his DAB account on the same day; and
- on 1 March 2015, $208,276 in cash was deposited into Customer 1's DAB account, then $700,000 was withdrawn from his DAB account by telegraphic transfer the following day.

Due diligence

By 1 March 2016, the due diligence steps taken with respect to Customer 1 included:

- searches conducted by the Credit control team in March 2010 for the purpose of assessing his creditworthiness before approving a credit facility with a limit of $10,000,000;
- in February 2014, due diligence checks following media reporting identifying alleged links between an associate and business partner of Customer 1 and organised crime. Although Customer 1's risk rating was increased to Significant, Crown did not record any further action in response to this information;
- a due diligence report was obtained by March 2014 which identified Customer 1 as a foreign PEP; and
- by January 2015, Crown obtained a wealth report on Customer 1, which named him as an alleged organised crime figure who held prominent political positions.

On 15 September 2015, an Australian broadcast program named Customer 1 and his junket, Suncity, and reported that an alleged organised crime figure was allegedly the ultimate beneficiary of the Suncity business. Following this, Crown prepared a list of individuals mentioned in the program for the purpose of considering further action, along with a list of Suncity agents, identifying that Customer 1 was a shareholder in Suncity and ran the junket in his own name at Crown. Crown did not record any further action in response.

738. At all relevant times, Customer 1 was a foreign PEP on the basis of a position held in a foreign political organisation since at least March 2014.

Particulars

By March 2014, Crown Melbourne obtained a due diligence report that identified Customer 1 as a foreign PEP.

At no point did Crown Perth identify Customer 1 as a foreign PEP.

739. As at 1 March 2016, Customer 1 should have been recognised by Crown Melbourne as a high risk customer by reason of the matters pleaded at paragraph 737 and as a result of his foreign PEP status pleaded in paragraph 738.

Particulars

Section 36(1)(a), (b) of the Act and Chapter 15 of the Rules.

740. At all times on and from 1 March 2016 to 5 June 2017, Customer 1 should have been recognised by Crown Melbourne as a high risk customer by reason of the matters pleaded at paragraphs 737, 738, 745 , 746, 747, 748, 749, 750, 751, 752, 754 and 760.

Particulars

Section 36(1)(a), (b) of the Act and Chapter 15 of the Rules.

741. Crown Melbourne did not rate Customer 1 as high risk until 5 June 2017.

Particulars

The Standard Part A Programs set out four levels of customer risk ratings that could be applied to customers. The risk ratings, in order of lowest to highest risk were: low (the default risk rating); moderate; significant; and high.

On 57 occasions between 30 June 2010 and 3 February 2014, Crown Melbourne assessed Customer 1 as moderate risk.

On 84 occasions between 5 February 2014 and 31 May 2017, Crown Melbourne assessed Customer 1 as significant risk.

On 162 occasions between 5 June 2017 and 12 October 2021, Crown Melbourne assessed Customer 1 as high risk.

742. As at 1 March 2016, Customer 1 should have been recognised by Crown Perth as a high risk customer by reason of the matters pleaded at paragraph 737 and as a result of his foreign PEP status pleaded in paragraph 738.

Particulars

Section 36(1)(a), (b) of the Act and Chapter 15 of the Rules.

743. At all times on and from 1 March 2016 to 28 July 2017, Customer 1 should have been recognised by Crown Perth as a high risk customer by reason of the matters pleaded at paragraph 737, 738, 746, 747, 748, 751, 752, 757 and 760.

Particulars

Section 36(1)(a), (b) of the Act and Chapter 15 of the Rules.

744. Crown Perth did not rate Customer 1 as high risk until 28 July 2017.

Particulars

At no point prior to 8 March 2016 did Crown Perth consider Customer 1's risk rating. On 8 March 2016, Crown Perth rated Customer 1's risk as low.

On 5 occasions between 28 July 2017 and 23 March 2020, Crown Perth assessed Customer 1 as high risk.

745. On and from 1 March 2016, designated services provided to Customer 1 at Crown Melbourne and Crown Perth posed higher ML/TF risks including because the provision of designated services to Customer 1 involved a combination of the following factors:

a. Customer 1 received high value financial and gaming services (tables 1 and 3, s6) through multiple junket programs: see paragraph 473ff;

b. Customer 1 facilitated the provision of high value financial and gaming services (tables 1 and 3, s6) to key players (including foreign PEPs such as Customer 45) on his junket programs: see paragraph 473ff;

c. Customer 1 was a junket operator and junket player;

d. Customer 1 was a foreign PEP: see paragraphs 118 and 738;

e. between 1 March 2016 and March 2020, Crown Melbourne recorded that total turnover on junkets run by Customer 1 at Crown Melbourne had exceeded $20,157,461,548;

f. between 1 March 2016 and February 2020, Crown Perth recorded that total turnover on junkets run by Customer 1 at Crown Perth had exceeded $2,115,419,720;

g. Customer 1 was known at all times to be connected to other junket operators, including the Chinatown junket, the Meg-Star junket, the Customer 4 junket and the Customer 2 junket;

h. designated services provided to Customer 1 lacked transparency as the services were provided through the channel of junket programs: see paragraph 477(e);

i. the table 3, s6 designated services provided to Customer 1 involved high turnover;

j. Customer 1 was provided with a substantial standing credit line with a limit of $30,000,000 to operate his junket programs, which was reapproved by Crown management on a monthly basis. From March 2019, the credit limit was increased to $50,000,000: see paragraphs 280ff and 487;

k. large values were transferred to and from Customer 1's DAB account, and then to and from other customers' DAB accounts, involving the provision by Crown Melbourne and Crown Perth of designated services within the meaning of items 31 and 32, table 1, s6 of the Act: see paragraphs 411ff and 492:

    i. for example, on 30 July 2019, Customer 2, who was also a junket operator, transferred $2,000,000 from his DAB account to Customer 1's DAB account at Crown Melbourne;

l. designated services provided to Customer 1 involved large transfers to and from third parties, including to and from other junket operators in respect of whom Crown Melbourne and Crown Perth had formed suspicions, foreign remittance service providers and unknown third parties: see paragraph 456ff:

    i. from 1 March 2016, Crown Melbourne gave the AUSTRAC CEO SMRs in relation to a number of telegraphic transfers from Customer 1 to third parties totalling $7,796,163; and

    ii. from 1 March 2016, Crown Melbourne gave the AUSTRAC CEO SMRs in relation to a number of telegraphic transfers from third parties to Customer 1 totalling $14,995,924.40;

m. designated services provided to Customer 1 involved large cross-border movements of funds, including through a Southbank account: see paragraph 239;

n. Customer 1 and his junket representatives engaged in transactions indicative of ML/TF typologies and vulnerabilities, including structuring, cashing in large value chips with no evidence of play and quick turnover of funds (without betting): see paragraph 24;

o. at various times in 2016, designated services provided to Customer 1 were indicative of the ML/TF typology of refining:

    i. in 2016, Crown Melbourne exchanged at least $661,900 presented in $50 notes for $100 notes on behalf of Customer 1 or key players on his junkets;

p. these transactions took place against the background of 99 SMRs being given to the AUSTRAC CEO by Crown Melbourne by 1 March 2016 with respect to Customer 1;

q. between 12 May 2016 and 29 September 2016, Crown Melbourne made available the Crown private jet for the use of Customer 1 and his Suncity junket on four occasions. There were inadequate controls on the carrying of large amounts of cash on Crown's private jets*:* see paragraphs 454 and 491(c);

r. in November 2016, Crown Melbourne was advised that Customer 1 was of interest to law enforcement;

s. by January 2017, senior management was provided with information alleging that Customer 1 was:

    i. a former organised crime member;

    ii. a foreign PEP;

    iii. linked to the receipt of $81,000,000 stolen from a central bank; and

    iv. associated with individuals linked to organised crime.

t. in June 2017, Crown identified Customer 1 as a foreign PEP, based on his role as a member of a foreign political organisation;

u. in 2017 and 2018, there was a significant escalation in the volume of suspicious large cash deposits and withdrawals at the Suncity cash administration desk in Crown Melbourne (see paragraph 529ff) made by Customer 1's junket representatives, key players and third parties, that were reported to the AUSTRAC CEO:

    i. persons associated with the Suncity junket transacted using large amounts of cash and cash that appeared suspicions, including large volumes of cash in small notes in rubber bands, plastic bags, shoe boxes and counterfeit cash at the Suncity cash administration desk: see paragraphs 450, 451, 452 and 491; and

    ii. from 1 March 2016 to December 2018, there were at least 75 suspicious incidents in the Suncity room involving cash, and known to Crown Melbourne, totalling at least $23,398,220;

v. in January 2018, Crown Melbourne received an enquiry from law enforcement in relation to a Suncity cash administration desk cash deposit by a key player, Customer 20, with suspected involvement from Customer 1;

w. in April 2018, Crown Melbourne received three more law enforcement enquiries in relation to Suncity cash administration desk cash deposits and other deposits into Customer 1's DAB account;

x. in April 2018, Crown staff discovered cash totalling approximately $5,600,000 at the Suncity cash administration desk in Crown Melbourne;

y. in May 2018, Crown management agreed to offset an AUD$9,600,000 debt owed by a Crown patron, Customer 27, against lucky money owed to Customer 1;

z. in December 2018, a key player on Customer 1's junket programs was arrested attempting to deposit $250,000 cash, provided to him by a Suncity staff member in the Crown Melbourne carpark, into a flagged account;

aa. in July and August 2019, media reports named Customer 1 as:

i. allegedly the subject of overseas law enforcement enquiries for engaging in illegal gambling;

ii. allegedly linked to organised crime,

iii. allegedly banned from entering Australia; and

iv. allegedly linked to money laundering through Australian casinos;

bb. at various times, Customer 1 had significant parked or dormant funds in his DAB accounts: see paragraph 252;

i. as at 18 June 2021, Customer 1 had parked $1,337,169 in his safekeeping account, which had not been transacted on since January 2021; and

cc. by reason of the matters pleaded at subparagraphs a. to bb., there were real risks that Customer 1's source of wealth and source of funds were not legitimate.

Monitoring of Customer 1's transactions

746. At no time did Crown Melbourne or Crown Perth appropriately monitor Customer 1's transactions on a risk-basis.

Particulars

Section 36(1)(a), (b) of the Act and rules 15.4 to 15.8 of the Rules.

Crown Melbourne and Crown Perth were unable to monitor the ML/TF risks posed by transactions associated with Customer 1's junkets, including transactions by his junket representatives and key players on his junkets, appropriately because they did not make and keep appropriate records of designated services provided: see paragraphs 483ff.

Crown Melbourne and Crown Perth did not apply appropriate risk-based transaction monitoring to designated services provided to Customer 1: see paragraphs 590ff and 629 to 642 (designated services) and 643 to 649 (transactions facilitated through junkets).

Suncity cash administration desk cash transactions

See paragraph 749 below.

Lookback

Customer 1's transactions involved repeated transactions indicative of ML/TF typologies that were not detected prior to 2021. Had appropriate risk-based transaction monitoring been applied, these transactions could have been identified earlier: see paragraphs 686 and 687.

Transactions indicative of ML/TF typologies – third party transfers

For example, an independent expert identified that from July 2019 to June 2020, Customer 1 received numerous third party deposits into his DAB account, including:

- between 2 July 2019 and 14 September 2019, Customer 1 received 9 payments from third parties through a Southbank account, totalling $623,876;
- between 2 October 2019 and 31 December 2019, Customer 1 received 42 payments from third parties through a Crown Patron account, totalling $9,877,307; and
- between 3 January 2020 and 9 June 2020, Customer 1 received 25 payments from third parties through a Crown Patron account, totalling $8,110,249.

By 15 October 2021, an independent auditor identified that:

- Customer 1 was one of the 14 patrons that had made payments to a common beneficiary;
- Customer 1 had made telegraphic transfers from Crown Melbourne and Crown Perth on 111 occasions between 7 April 2014 and 19 March 2020, in an amount totalling $142,035,550.12; and
- Customer 1 had made 111 payments to 53 unique third parties, to a total value of $53,060,828.

Transactions indicative of ML/TF typologies – quick turnover of funds (without betting)

By 15 October 2021, an independent auditor identified that Customer 1 was one of the eleven patrons responsible for 66% of the total value of identified quick turnover of funds (without betting) transactions, despite being only 22% of the total instances.

Inadequate controls on Crown's private jets

On 12 May 2016, Crown Melbourne provided Customer 1 with access to a Crown private jet to facilitate travel from one foreign country to another foreign country.

On 13 May 2016, Crown Melbourne provided Customer 1 with access to a Crown private jet to facilitate travel from a foreign country to Melbourne for 12 people.

On 19 May 2016, Crown Melbourne provided Customer 1 with access to a Crown private jet to facilitate travel from Melbourne to a foreign country for 12 people.

On 29 September 2016, Crown Melbourne provided the Suncity junket with access to a Crown private jet to facilitate travel from a foreign country to Perth for 12 people.

There were inadequate controls on the carrying of large amounts of cash on Crown's private jets*:* see paragraphs 454 and 491(c).

Ongoing customer due diligence

747. On and from 1 March 2016, on multiple occasions, the provision of designated services to Customer 1 at Crown Melbourne and Crown Perth raised red flags reflective of higher ML/TF risks as a result of Customer 1's junket activity.

Particulars

See paragraph 477.

Total gaming activity on junket programs run by Customer 1 from March 2016 to March 2020

Between March 2016 and March 2020, Customer 1 had operated at least 115 junket programs at Crown Melbourne. Crown Melbourne recorded total turnover of approximately $20,157,461,548, and losses of approximately $363,660,405. Commissions of approximately $211,187,591 were payable by Crown Melbourne to Customer 1.

Between March 2016 and March 2020, Customer 1 had operated at least 76 junket programs at Crown Perth. Crown Perth recorded total turnover of approximately $2,115,419,720, and losses of approximately $71,744,133. Commissions of $25,357,032 were payable by Crown Perth to Customer 1.

Junket activity in 2016

Crown Melbourne recorded that gaming activity on junket programs run by Customer 1 at Crown Melbourne during the 2016 financial year involved turnover of approximately $2,355,476,000, with losses of approximately $16,555,841. Commissions of approximately $9,933,505 were payable by Crown Melbourne to Customer 1.

Crown Perth recorded that gaming activity on junket programs run by Customer 1 at Crown Perth during the 2016 financial year involved turnover of approximately $43,977,200, with wins of approximately $2,773,980.

Between 1 March 2016 and 1 December 2016, Crown Melbourne was aware of the high losses noted for the key players under Suncity junket programs, giving the AUSTRAC CEO 12 SMRs that described losses by 56 key players under Suncity junkets totalling AUD$33,423,635, and separately HKD25,145,000: two SMRs dated 1 March 2016, SMR dated 1 April 2016, SMR dated 2 May 2016, SMR dated 31 May 2016, SMR dated 5 July 2016, SMR dated 1

August 2016, SMR dated 1 September 2016, SMR dated 3 October 2016, SMR dated 2 November 2016, and two SMRs dated 1 December 2016.

Between April 2016 and December 2016, Crown management regularly reapproved Customer 1's credit facility, to a limit of AUD$30,000,000, as part of a monthly junket review.

Junket activity in 2017

During the 2017 financial year, Customer 1 operated at least 25 junket programs at Crown Melbourne. Crown Melbourne recorded the total turnover for those programs was approximately $3,002,691,767, with losses of approximately $52,066,588. Commissions of approximately $31,289,012 were payable by Crown Melbourne to Customer 1.

During the 2017 financial year, Customer 1 operated at least 20 junket programs at Crown Perth. Crown Perth recorded the total turnover for those programs was approximately $128,811,705, with losses of approximately $4,404,029. Commissions of approximately $2,660,412 were payable by Crown Perth to Customer 1.

Between 3 January 2017 and 6 December 2017, Crown Melbourne was aware of the high losses noted for the key players under Suncity junket programs, giving the AUSTRAC CEO 14 SMRs that described losses by 59 key players under Suncity junkets totalling $44,044,880, and separately HKD101,287,800: two SMRs dated 3 January 2017, SMR dated 2 February 2017, SMR dated 1 March 2017, SMR dated 3 April 2017, SMR dated 1 May 2017, SMR dated 2 August 2017, SMR dated 31 August 2017, SMR dated 1 September 2017, SMR dated 2 October 2017, two SMRs dated 2 November 2017, SMR dated 1 December 2017, and SMR dated 6 December 2017.

Between January 2017 and December 2017, Crown management regularly reapproved Customer 1's junket credit facility, to a limit of AUD$30,000,000, as part of a monthly junket review.

Junket activity in 2018

During the 2018 financial year, Customer 1 operated at least 24 junket programs at Crown Melbourne. Crown Melbourne recorded the total turnover for those programs was approximately $7,286,784,197, with losses of approximately $126,487,006. Commissions of $80,370,709 were payable by Crown Melbourne to Customer 1.

During the 2018 financial year, Customer 1 operated at least 11 junket programs at Crown Perth. Crown Perth recorded the total turnover for those programs was approximately $72,231,068, with losses of approximately $656,370. Commissions of approximately $313,169 were payable by Crown Perth to Customer 1.

Between 1 February 2018 and 1 August 2018, Crown Melbourne was aware of the high losses noted for the key players under Suncity junket programs, giving the AUSTRAC CEO 12 SMRs that described

losses by 62 key players under Suncity junkets totalling $41,419,635, and separately HKD150,592,000: two SMRs dated 1 February 2018, two SMRs dated 1 March 2018, two SMRs dated 3 April 2018, two SMRs dated 1 May 2018, SMR dated 1 June 2018, two SMRs dated 2 July 2018, and SMR dated 1 August 2018.

Between January 2018 and December 2018, Crown management regularly reapproved Customer 1's junket credit facility, to a limit of AUD$30,000,000, as part of a monthly junket review.

Junket activity in 2019

During the 2019 financial year, Customer 1 operated at least 25 junket programs at Crown Melbourne. Crown Melbourne recorded the total turnover for those programs was approximately $4,426,941,528 with losses of approximately $76,640,443. Commissions of approximately $44,798,893 were payable by Crown Melbourne to Customer 1.

During the 2019 financial year, Customer 1 operated at least 25 junket programs at Crown Perth. Crown Perth recorded the total turnover for those programs was approximately $225,333,300, with losses of approximately $7,945,025. Commissions of approximately $3,273,460 were payable by Crown Perth to Customer 1.

Between January 2019 and March 2019, Crown management regularly reapproved Customer 1's junket credit facility, to a limit of AUD$30,000,000, as part of a monthly junket review.

From approximately 6 March 2019 to December 2019, Crown management agreed to increase Customer 1's credit facility to $50,000,000.

Junket activity in 2020

Between January 2020 and March 2020, Crown management regularly reapproved Customer 1's junket credit facility, to a limit of AUD$50,000,000, as part of a monthly junket review.

Customer 1 continued to run junkets until March 2020, when the COVID-19 pandemic restrictions took effect.

During the 2020 financial year, Customer 1 operated at least 33 junket programs at Crown Melbourne. Crown Melbourne recorded the total turnover for those programs was approximately $3,088,650,897, with losses of approximately $55,705,966. Commissions of approximately $32,769,867 were payable by Crown Melbourne to Customer 1.

During the 2020 financial year, Customer 1 operated at least 15 junket programs at Crown Perth. Crown Perth recorded the total turnover for those programs was approximately $40,476,437 with losses of approximately $440,651. Commissions of approximately $121,335 were payable by Crown Perth to Customer 1.

748. On and from 1 March 2016, on multiple occasions, the provision of designated services to Customer 1 at Crown Melbourne and Crown Perth raised red flags reflective of higher ML/TF risks as a result of unusual transactions and patterns of transactions involving Customer 1.

Particulars

Unusual transactions and patterns of transactions in 2016

Over the course of 2016, designated services provided to Customer 1 included complex, unusual large transactions involving key players on his junkets (such as Customer 20) and other third parties depositing or withdrawing funds from Customer 1's DAB account, and transactions indicative of ML/TF typologies, including quick turnover of funds (without betting), refining, and suspicious cash transactions: see paragraphs 24, 420ff, 456ff, 450, 451, 491.

In April and May 2016, Customer 1 engaged in transactions indicative of ML/TF typologies involving quick turnover of funds (without betting), in which money was deposited into Customer 1's DAB account by telegraphic transfer, and then withdrawn from his DAB account on the same day.

On 22 June 2016, Customer 1 arranged for two international telegraphic transfers to two third parties of $2,511,575 and $260,000: SMR dated 23 June 2016.

In July 2016, Customer 1 engaged in transactions indicative of ML/TF typologies involving quick turnover of funds, in which money was deposited into Customer 1's DAB account by telegraphic transfer, and then withdrawn from his DAB account on the same day.

On 18 July 2016, Customer 1 received a telegraphic transfer of $20,000 into his Crown Melbourne DAB account from a third party, Person 59, who was not a key player under any Suncity junket programs: SMR dated 19 July 2016.

On 5 October 2016, a third party, Person 16, deposited $480,000 into the Crown Melbourne DAB account of a key player on the Suncity junket, Customer 20. The funds were subsequently transferred into Customer 1's Crown Melbourne DAB account: SMR dated 6 October 2016.

On 23 October 2016, Customer 1 arranged an international telegraphic transfer of $70,000 from Crown Melbourne to a third party, Person 16: SMR dated 24 October 2016.

On 26 October 2016, a key player, Customer 25, exchanged $411,900 of $50 notes for $100 notes on behalf of Customer 1 at the Suncity cash administration desk. Crown Melbourne discovered that three of these notes were counterfeit: SMR dated 27 October 2016. This transaction was indicative of the ML/TF typology of refining.

On 31 October 2016, two telegraphic transfers totalling $40,000 from a third party were deposited into Customer 1's Crown Melbourne

DAB account, despite the individual not being listed as a key player under any Suncity junket programs: SMR dated 2 November 2016.

On 6 November 2016, an unknown representative of the Suncity junket exchanged $250,000 in $50 for $100 notes at the Suncity cash administration desk, with the cash appearing to originate from Customer 20, a key player on Customer 1's junket: SMR dated 7 November 2016. This transaction was indicative of the ML/TF typology of refining.

On 9 November 2016, a telegraphic transfer of $200,000 from a third party and Person 46, who were not listed as key players under any Suncity junket programs, was deposited into Customer 1's Crown Melbourne account: SMR dated 10 November 2016.

On 9 December 2016, a telegraphic transfer of $80,000 from a third party, who was not listed as a key player under any Suncity junket programs, was deposited into Customer 1's Crown Melbourne DAB account: SMR dated 10 December 2016.

Unusual transactions and patterns of transactions in 2017

Over the course of 2017, designated services provided to Customer 1 included complex, unusual large transactions on his DAB account involving key players on his junkets (including Customer 20, and Customer 23) and other third parties, and transactions indicative of ML/TF typologies, including quick turnover of funds (without betting) and suspicious cash transactions: see paragraphs 420ff, 456ff, 450,451 and 491.

On 24 February 2017, a telegraphic transfer of $100,000 was arranged by Customer 1 from his Crown Melbourne DAB account to a third party, with a comment stating that the winnings are from key player Customer 20: SMR dated 27 February 2017.

On 15 March 2017, a telegraphic transfer of $50,000 was arranged from Customer 1's Crown Melbourne DAB account, on behalf of key player Customer 20, to a third party, Person 43: SMR dated 17 March 2017.

On 23 March 2017, a telegraphic transfer of $200,000 was arranged by Customer 1 from his Crown Melbourne DAB account to a third party, with a comment stating that this transfer was arranged on behalf of a key player: SMR dated 24 March 2017.

On 26 April 2017, two telegraphic transfers of $37,000 and $100,000 were deposited into Customer 1's Crown Melbourne DAB account by two third parties: SMR dated 27 April 2017.

On 11 May 2017, a telegraphic transfer of $17,680 from third party was deposited into Customer 1's Crown Melbourne DAB account: SMR dated 12 May 2017.

On 30 May 2017, a telegraphic transfer of $81,000 from a third party was deposited into Customer 1's Crown Melbourne DAB account. On

31 May 2017, an additional telegraphic transfer of $17,985 was received from a third party, Person 59, into Customer 1's Crown Melbourne DAB account. Neither were key players under the Suncity junket: SMR dated 31 May 2017.

On 20 June 2017, a telegraphic transfer of $50,000 was arranged by Customer 1 from his DAB account at Crown Melbourne to a third party, Person 43: SMR dated 22 June 2017.

On 31 July 2017, a telegraphic transfer of $170,000 from Company 1 (a money changer) was deposited into the Crown Melbourne DAB account of Suncity key player, Customer 23. These funds were subsequently transferred to Customer 1's Crown Melbourne account: SMR dated 21 September 2017.

On 16 and 17 November 2017, a key player on the Suncity junket telegraphic transferred $200,000 from her Australian bank account to her Crown Melbourne DAB account, then transferred these funds to Customer 1's DAB account: SMR dated 1 December 2017.

On 29 November 2017, a third party, Person 16, deposited $893,000 by telegraphic transfer to the DAB account of Customer 1's key player, Customer 20. These funds were then transferred to Customer 1's Crown Melbourne DAB account: SMR dated 1 December 2017.

Unusual transactions and patterns of transactions in 2018

Over the course of 2018, at the same time as the suspicious cash deposits at the Suncity cash administration desk (see paragraph 749), other large unusual transactions were being conducted on Customer 1's DAB account, or by Customer 1's key players or third parties in connection with Customer 1: see paragraphs 420ff, 450,451, 456, and 491.

On 1 January 2018, Customer 22 presented $300,000 in cash in in three separate plastic bags with the notations "16/12/2017", "Mel" and "Jacey" and advised that he obtained the cash from the Suncity junket: SMR dated 2 January 2018;

On 16 January 2018, $60,000 was telegraphic transferred from Customer 1's Crown Melbourne DAB account to a third party, Person 43, with a comment that the transfer was on behalf of key player, Customer 20, for "payment of winnings": SMR dated 17 January 2018.

On 13 February 2018, Customer 1 received two telegraphic transfers into his Crown Melbourne DAB account from two third parties who were not key players under any Suncity junket programs, totalling $400,000 and $60,000: SMR dated 14 February 2018.

On 23 February 2018, a telegraphic transfer of $60,000 from the Crown Perth DAB account of a third party, who was not noted as a key player on any Suncity junkets, was deposited into Customer 1's Crown Melbourne DAB account: SMR dated 23 February 2018.

On 1 March 2018, a third party arranged for Crown Perth to telegraphic transfer $70,000 from his Crown Perth DAB account to Customer 1's DAB account at Crown Melbourne, despite not being noted as a key player on the Suncity junkets: SMR dated 9 March 2018.

On 14 March 2018, a telegraphic transfer of $500 was arranged by Customer 1 from his Crown Melbourne DAB account to a third party: SMR dated 15 March 2018.

On 15 March 2018, a telegraphic transfer of $800,000 was arranged by Customer 1 from his Crown Melbourne DAB account to a third party, Person 16: SMR dated 16 March 2018.

On 17 March 2018 and 18 March 2018, two telegraphic transfers were deposited from a third party to a key player on the Suncity junket totalling $199,500. The funds were transferred to Customer 1's Crown Melbourne DAB account: SMR dated 19 March 2018.

On 22 March 2018, a telegraphic transfer of $20,000 from a third party, who was not a key player under any of the Suncity junkets, was deposited into Customer 1's Crown Melbourne DAB account: SMR dated 23 March 2018.

On 26 March 2018, a telegraphic transfer of $85,000 from Person 46, a third party who was not a key player under any of the Suncity junkets, was deposited into Customer 1's Crown Melbourne DAB account: SMR dated 27 March 2018.

On 27 March 2018, a telegraphic transfer of $95,000 from Person 46, a third party who was not a key player under any of the Suncity junkets, was deposited into Customer 1's Crown Melbourne DAB account: SMR dated 28 March 2018.

An independent auditor identified that on 28 March 2018, Customer 1 engaged in transactions indicative of ML/TF typologies involving quick turnover of funds (without betting), in which $95,000 and $85,000 was deposited into Customer 1's DAB account by telegraphic transfer, and then $1,500,000 was withdrawn in cash from his DAB account the following day.

On 30 March 2018, a telegraphic transfer of $174,000 was deposited into a Meg-Star junket representative's Crown Melbourne DAB account. The funds were subsequently transferred to Customer 1's DAB account: SMR dated 3 August 2018.

On 18 April 2018, a telegraphic transfer of $300,000 was arranged by Customer 1 from his Crown Melbourne DAB account to a third party, Person 16: SMR dated 19 April 2018.

Following the implementation of cash controls at the Suncity cash administration desk (see paragraph 529ff), unusual transactions through Customer 1's DAB account, or involving Customer 1's key players or junket representatives, continued.

On 3 May 2018, a telegraphic transfer of $50,000 was arranged by Customer 1 from his Crown Melbourne DAB account to a third party: SMR dated 4 May 2018.

On 8 May 2018, a telegraphic transfer of $800,000 was arranged by Customer 1 from his Crown Melbourne DAB account to a third party, Person 16: SMR dated 9 May 2018.

On the following occasions in May 2018, Customer 1 engaged in transactions indicative of ML/TF typologies involving quick turnover of funds (without betting), including:

- on 5 May 2018, $69,000 was deposited into Customer 1's DAB account in cash, then $350,000 was withdrawn by telegraphic transfer and $50,000 was withdrawn in cash from his DAB account on the same day;
- on 9 May 2018, $200,000 was deposited into Customer 1's DAB account by telegraphic transfer, and then $10,000, $9,000, $5,000, and $70,000 was withdrawn in cash from his DAB account the same day. Two days later, on 11 May 2018, $125,000, $40,000 and $10,000 was withdrawn in cash from his DAB account;
- on 16 May 2018, $20,000 was deposited into Customer 1's DAB account by telegraphic transfer, then $3,000 in cash and $26,600 by telegraphic transfer was withdrawn from his DAB account on the same day. A day later, on 17 May 2018, a further $20,000 was withdrawn in cash from his DAB account;
- on 29 May 2018, $100,000 was deposited into Customer 1's DAB account in cash, then $3,100 and $83,900 was withdrawn by telegraphic transfer from his DAB account on the same day. A day later, a further $250,000, $19,000 and $10,000 was withdrawn in cash from his DAB account; and
- on 31 May 2018, $35,000 was deposited into Customer 1's DAB account in cash, then $5,600,000 was withdrawn by telegraphic transfer from his DAB account on the same day.

On 4 June 2018, $15,000 was withdrawn in cash from Customer 1's DAB account by Customer 1's junket representative, ostensibly for a Suncity key player, but ultimately provided to a third party, Person 31, who had no known affiliation with the Suncity junket: SMR dated 6 June 2018.

On 15 June 2018, a key player on the Suncity junket deposited $200,000 cash into Customer 1's Crown Melbourne DAB account: SMR dated 18 June 2018.

On the following occasions in June 2018, Customer 1 engaged in transactions indicative of ML/TF typologies involving quick turnover of funds (without betting), including:

- on 15 June 2018, $200,000 was deposited into Customer 1's DAB account in cash, then $20,000 and $25,000 was withdrawn in cash from his DAB account on the same day. The following day, on 16 June 2018, a further $577,900 was withdrawn by telegraphic transfer from his DAB account on the same day; and
- on 28 June 2018, $29,970 was deposited into Customer 1's DAB account in cash and $580,000 was deposited by telegraphic transfer, then $70, $35,000 and $50,000 was withdrawn in cash on the same day. The following day, on 29 June 2018, a further $300,000 was withdrawn by telegraphic transfer, and $150,000 and $25,000 was withdrawn in cash from his DAB account.

On 5 July 2018, a telegraphic transfer of $44,438 was arranged by Customer 1 from his Crown Melbourne DAB account to the Australian bank account of a third party who was not listed as a key player under any of the Suncity junkets: SMR dated 6 July 2018.

On 18 July 2018, a telegraphic transfer of $20,000 from a third party, who was not listed as a key player under any of the Suncity junkets, was deposited into Customer 1's Crown Melbourne DAB account: SMR dated 19 July 2018.

On 20 July 2018, a further telegraphic transfer of $20,000 from the same third party as immediately above, who was not listed as a key player under any of the Suncity junkets, was deposited into Customer 1's Crown Melbourne DAB account: SMR dated 23 July 2018.

On the following occasions in July 2018, Customer 1 engaged in transactions indicative of ML/TF typologies involving quick turnover of funds (without betting), including:

- on 6 July 2018, $20,000 and $20,000 was deposited into Customer 1's DAB account by telegraphic transfer, then $26,900 and $100,000 was withdrawn in cash from his DAB account on the same day;
- on 7 July 2018, $20,000 and $20,000 was deposited into Customer 1's DAB account by telegraphic transfer, then $10,000, $20,000 and $50,000 was withdrawn in cash from his DAB account on the same day. The following day, a further $700,000 was withdrawn by telegraphic transfer and $38,250, $23,895 and $10,000 was withdrawn in cash from his DAB account;
- on 11 July 2018, $20,000 by telegraphic transfer and $5,000 in cash was deposited into Customer 1's DAB account, then $14,500, $20,000 and $75,750 was withdrawn in cash from his DAB account on the same day. The following days, a further $30,000 (12 July 2018) and $50,000 and $4,000 (13 July 2018) was withdrawn in cash from his DAB account;
- on 16 July 2018, four deposits of $20,000 were made by telegraphic transfer into Customer 1's DAB account, and a further

$10,000 and $60,250 was withdrawn in cash from his DAB account on the same day;

- on 18 July 2018, $10,000 in cash and $20,000 by telegraphic transfer was deposited into Customer 1's DAB account, then $40,000 was withdrawn in cash from his DAB account on the same day. Two days later, on 20 July 2018, a further $116,000, $100,000 and $8,500 in cash was withdrawn from his DAB account;
- on 21 July 2018, $20,000 by telegraphic transfer was deposited into Customer 1's DAB account. The following day, $16,000 was withdrawn in cash from his DAB account;
- on 24 July 2018, $20,000 by telegraphic transfer was deposited into Customer 1's DAB account, then $30,000 was withdrawn in cash from his DAB account on the same day; and
- on 28 July 2018, $20,000 by telegraphic transfer was deposited into Customer 1's DAB account. The following day, $72,300 by telegraphic transfer and $35,900 in cash was withdrawn from his DAB account. On 30 July 2018, a further $21,000 in cash was withdrawn from his DAB account.

On 1 August 2018, $200,000 worth of winnings was paid out in cash from Customer 1's Crown Melbourne DAB account to a key player on the Suncity junket. The following day, the key player requested that the funds instead be telegraphically transferred to his nominated bank account, which was denied, so cash in the amount of $180,000 was deposited back into Customer 1's Crown Melbourne DAB account. On 3 August 2018, a telegraphic transfer of $129,650 was recorded from Customer 1's Crown Melbourne DAB account, on behalf of key player, to a third party: SMR dated 3 August 2018.

On 3 August 2018, two telegraphic transfers were deposited into Customer 1's DAB account from third parties, including $80,000 from a first third party and $10,000 from a second third party: SMR dated 6 August 2018.

On 13 August 2018, a representative for the Suncity junket presented $80,000 at the Pit 38 buy-in window, on behalf of a key player on the Suncity junket, Customer 25, to be deposited into Customer 1's Crown Melbourne DAB account. The funds were allegedly from an unknown money changer and brought in by Customer 25's personal assistant. Crown employees discovered and confiscated five counterfeit $100 notes and deposited the remaining $79,500 into Customer 1's Crown Melbourne DAB account: SMR dated 14 August 2018.

Between 14 August 2018 and 22 August 2018, a third party, who was not noted as a key player under any Suncity junket programs, Person 49, made the following telegraphic transfers totalling $1,489,590.40:

- on 14 August 2018, two telegraphic transfers totalling $689,590.40 from the third party were deposited into Customer 1's Crown Melbourne DAB account. Shortly afterwards, a telegraphic transfer of $100,000 was arranged from Customer 1's Crown Melbourne DAB account to another third party: SMR dated 15 August 2018;
- on 21 August 2018, a telegraphic transfer of $400,000 deposited into Customer 1's Crown Melbourne DAB account: SMR dated 22 August 2018; and
- on 22 August 2018, a telegraphic transfer of $400,000 deposited into Customer 1's Crown Melbourne DAB account: SMR dated 23 August 2018.

On 24 August 2018, three telegraphic transfers totalling $260,000 from a third party, who was not noted as a key player under any Suncity junket programs, were deposited into Customer 1's Crown Melbourne DAB account: SMR dated 27 August 2018.

On 29 August 2018, a telegraphic transfer of $130,000 was arranged by Customer 1 from Crown Melbourne to a third party, who was not noted as a key player under any Suncity junket programs: SMR dated 30 August 2018.

On the following occasions in August 2018, Customer 1 engaged in transactions indicative of ML/TF typologies involving quick turnover of funds (without betting), including:

- on 8 August 2018, $100,000 in cash, and $10,000 and $10,000 by telegraphic transfer was deposited into Customer 1's DAB account, then $20,000 in cash was withdrawn from his DAB account on the same day. The following day, on 9 August 2018, a further $90,000 in cash was withdrawn from his DAB account;
- on 25 August 2018, $87,000 by telegraphic transfer was deposited into Customer 1's DAB account, then $31,000 in cash was withdrawn from his DAB account on the same day. The following day, on 26 August 2018, a further $70,000, $38,000 and $25,000 in cash was withdrawn from his DAB account; and
- on 30 August 2018, $87,000 was deposited into Customer 1's DAB account by telegraphic transfer. The following day, on 31 August 2018, $100,000 and $10,000 in cash was withdrawn from his DAB account.

On 4 September 2018, a telegraphic transfer of $200,000 from third party, Person 49, who was not noted as a key player under any Suncity junket programs, was deposited into Customer 1's DAB account at Crown Melbourne: SMR dated 5 September 2018.

On 7 September 2018, a telegraphic transfer of $200,000 was arranged from Customer 1's DAB account at Crown Melbourne to a third party, who was not noted as a key player under any Suncity junket programs: SMR dated 10 September 2018.

Between 18 September 2018 and 19 September 2018, four telegraphic transfers from four third parties were deposited into Customer 1's DAB account at Crown Melbourne, totalling $604,200: SMR dated 20 September 2018.

On 26 September 2018, a telegraphic transfer of $108,000 from third party, who was not noted as a key player for Customer 1, but was a junket representative for another junket operator, was deposited into Customer 1's DAB account at Crown Melbourne: SMR dated 27 September 2018.

On the following occasions in September 2018, Customer 1 engaged in transactions indicative of ML/TF typologies involving quick turnover of funds (without betting), including:

- on 6 September 2018, $200,000 was deposited into Customer 1's DAB account by telegraphic transfer, then $5,000 and $50,000 in cash was withdrawn from his DAB account on the same day. The following day, a further $200,000 by telegraphic transfer and $30,000 and $30,000 in cash was withdrawn from his DAB account. On 8 September 2018, a further $160,000 by telegraphic transfer and $52,940 in cash was withdrawn from his DAB account;
- on 24 September 2018, $60,000 in cash was deposited into Customer 1's DAB account, then $45,000 and $60,000 in cash, and $1,100,000 by telegraphic transfer was withdrawn from his DAB account on the same day. The following day, on 25 September 2018, a further $60,000 in cash was withdrawn from his DAB account; and
- on 29 September 2018, $50,000 in cash and $12,335 by telegraphic transfer was deposited into Customer 1's DAB account, then $100,000 in cash was withdrawn from his DAB account on the same day. Two days later, on 1 October 2018, a further $66,000 in cash was withdrawn from his DAB account.

On 5 October 2018, Customer 1 engaged in transactions indicative of ML/TF typologies involving quick turnover of funds (without betting), in which $200,000 in cash was deposited into Customer 1's DAB account, then the following day, on 6 October 2018, $60,000, $50,000, $35,000 and $25,000 in cash, and $25,000 by telegraphic transfer was withdrawn from his DAB account.

On 8 October 2018, Customer 1's junket representative, Person 29, deposited $300,000 in cash into Customer 1's DAB account to cover his losses under the Suncity junket program: SMR dated 10 October 2018.

On 12 November 2018, a Crown patron and junket operator transferred $100,000 from his Crown Melbourne DAB account to his Crown Perth DAB account for the purpose of front money for play on a program, but his gaming recorded on the program was minimal. During this time, this patron was also listed as a key player on

Customer 1's Crown Perth junket program, of which the patron's brother was a junket representative. On 20 November 2018, this patron arranged for Crown Perth to telegraphic transfer the funds back to Crown Melbourne, to the DAB account of another junket operator, Person 20: SMR dated 23 November 2018 (Crown Perth).

On 23 November 2018, a telegraphic transfer of $90,000 from a third party, who was not noted as a key player under the Suncity junket programs, was deposited into Customer 1's DAB account: SMR dated 26 November 2018.

Between October 2018 and December 2018, there were a series of suspicious cash transactions involving five identical cash deposits of $200,000 presented in $50 notes from third parties into Customer 1's DAB account, totalling $1,000,000:

- on 22 October 2018, a key player under the Suncity junket, deposited $200,000 cash in $50 notes into Customer 1's DAB account, claiming that he got the cash from home: SMR dated 23 October 2018;
- on 5 November 2018, a key player under the Suncity junket, presented at the Pit 86 buy-in window and deposited $200,000 cash in $50 notes into Customer 1's DAB account in exchange for chips, claiming that he got the cash from home: SMR dated 7 November 2018;
- on 11 November 2018, a key player under the Suncity junket exchanged $200,000 cash presented in $50 notes for chips: SMR dated 12 November 2018;
- on 29 November 2018, a junket representative for Customer 1 presented a bag containing $200,000 cash in $50 notes on behalf of a key player, claiming that the key player obtained them from home: SMR dated 30 November 2018; and
- on 7 December 2018, a Suncity staff member and a key player on the Suncity junket presented a bag containing $200,000 cash in $50 notes, claiming that the key player obtained them from home: SMR dated 7 December 2018.

Unusual transactions and patterns of transactions in 2019

In 2019, further suspicious amounts of cash were deposited, including counterfeit notes, and transactions indicative of ML/TF typologies were conducted on Customer 1's DAB account: see paragraphs 24, 450,451 and 491.

Between 6 and 9 February 2019, transactions in Customer 1's DAB account were indicative of the ML/TF typology of structuring, made up of six transactions of $5,000, $2,500, $5,000, $5,000, $2,000 and $3,000.

On 9 January 2019, Customer 1's junket representative deposited $100,000 cash presented in a bag with Crown branding in $50 notes into Customer 1's DAB account: SMR dated 10 January 2019.

On 20 February 2019, a key player on the Suncity junket deposited $190,000 in cash into Customer 1's DAB account, which included 3 counterfeit notes: SMR dated 21 February 2019.

On 5 March 2019, a telegraphic transfer of $147,294 from a third party, who was not a key player under any Suncity junket programs, was deposited into Customer 1's DAB account: SMR dated 6 March 2019.

On 13 March 2019, a telegraphic transfer of $305,000 from a third party, who was not a key player under any Suncity junket programs, was deposited into Customer 1's DAB account at Crown Melbourne: SMR dated 14 March 2019.

On 18 March 2019, four telegraphic transfers totalling $1,000,000 from four third parties (including Person 9, Person 15 and Person 17), who were not key players of the Suncity junket, were deposited into Customer 1's DAB account. The SMR identified that the third parties were the same individuals involved in telegraphic transfers for the Customer 2 junket: SMR dated 19 March 2019.

On 19 March 2019, a telegraphic transfer of $20,000 from a third party, who was not noted as a key player under any Suncity junket programs, was deposited into Customer 1's DAB account at Crown Melbourne: SMR dated 20 March 2019.

On 21 March 2019, two telegraphic transfers from two third parties who were not noted as key players under any Suncity junket programs (Person 9 and another third party) totalling $200,000 were deposited into Customer 1's DAB account at Crown Melbourne: SMR dated 22 March 2019.

On 27 March 2019, a telegraphic transfer of $20,000 from a third party who was not noted as a key player under any Suncity junket programs, was deposited into Customer 1's DAB account at Crown Melbourne: SMR dated 28 March 2019.

On the following occasions in March 2019, Customer 1 engaged in transactions indicative of ML/TF typologies involving quick turnover of funds (without betting), including:

- on 12 March 2019, $44,908 in cash was deposited into Customer 1's DAB account, then $44,908 in cash and $280,000 by telegraphic transfer was withdrawn from his DAB account; and
- on 19 March 2019, $20,000 by telegraphic transfer was deposited into Customer 1's DAB account, then $20,000 and $50,000 in cash was withdrawn from his DAB account.

On 3 April 2019, a telegraphic transfer of $20,000 from a third party, who was not noted as a key player under any Suncity junket

programs, was deposited into Customer 1's DAB account at Crown Melbourne: SMR dated 4 April 2019.

Between 8 April 2019 and 13 May 2019, transactions in Customer 1's DAB account were indicative of the ML/TF typology of structuring, made up of nine transactions of $100, $1000, $8900, $100 and $4000, $3000, $9000, $9800, and $9000.

On 17 April 2019, a telegraphic transfer of $20,000 from a third party who was not noted as a key player under any Suncity junket programs, was deposited into Customer 1's DAB account at Crown Melbourne: SMR dated 18 April 2019.

On 23 April 2019, a telegraphic transfer of $100,000 from Person 45, a third party who was not noted as a key player under any Suncity junket programs, was deposited into Customer 1's DAB account at Crown Melbourne: SMR dated 26 April 2019.

Between 5 and 21 May 2019, 8 sets of $50,000 telegraphic transfers by a third party, but believed by Crown to be for a key player on the Suncity junket, were deposited into Customer 1's DAB account, totalling $400,000: SMRs dated 7 May 2019; 10 May 2019; 16 May 2019; and 22 May 2019.

On 24 May 2019, three telegraphic transfers totalling $2,000,000 by a third party, Person 16, but believed by Crown to be for Customer 20, although he was not a current key player, were received by Crown Melbourne. Two of the payments were deposited into Customer 1's DAB account after Crown Melbourne received a letter stating that the funds were for gaming despite having a reference "payment to supplier", totalling $1,307,000; with the remaining payment returned to the third party as it contained a reference to "payment to supplier": SMRs dated 24 May 2019 and 28 May 2019.

On 28 May 2019, a telegraphic transfer of $15,800 from a third party who was not noted as a key player under any Suncity junket programs, was deposited into Customer 1's DAB account: SMR dated 29 May 2019.

On 5 June 2019, an international fund transfer of $693,000 from a third party, Person 16, but believed by Crown to be for Customer 20, although he was not a current key player, was deposited into Customer 1's DAB account at Crown Melbourne: SMR dated 6 June 2019.

On 12 June 2019, a set of two telegraphic transfers totalling $16,600 from a third party, who was not noted as a key player under any Suncity junket programs, were deposited into Customer 1's DAB account at Crown Melbourne: SMR dated 13 June 2019.

On 13 July 2019, a telegraphic transfer of $273,875 from a third party, who was not noted as a key player under any Suncity junket programs, was deposited into Customer 1's DAB account at Crown Melbourne: SMR dated 15 July 2019.

On 16 July 2019, two telegraphic transfers from two third parties, who were not noted as key players under any Suncity junket programs, were deposited into Customer 1's DAB account at Crown Melbourne, totalling $37,600: SMR dated 18 July 2019.

Between 17 and 19 July 2019, a key player listed on the Suncity junket at Crown Perth, Person 35, engaged in a series of transactions not supported by gaming activity on the Suncity junket, including depositing chips worth $15,600 into his Crown Perth DAB account, then withdrawing $5,600 in cash on 17 July 2019, then depositing $10,000 in cash into his Crown Perth DAB account, then arranging for Crown Perth to telegraphic transfer $20,000 to his foreign bank account, despite the amounts not corresponding to recorded play.

On 18 July 2019, Customer 1's junket representative withdrew $200,000 in cash for two key players, both of whom were winning under the junket program at Crown Melbourne. Approximately 15 minutes later, another Crown patron presented $200,000 in cash which appeared identical to the money previously cashed out (same seals and straps), for deposit into her DAB account, which raised suspicions of fund sharing or money lending: SMR dated 18 July 2019.

On 24 July 2019, two telegraphic transfers from two third parties, who were not noted as key players under any Suncity junket programs, were deposited into Customer 1's DAB account at Crown Melbourne, totalling $50,000: SMR dated 25 July 2019.

July 2019 DAB transfer between junket operators

On 30 July 2019, Customer 2 transferred $2,000,000 from his DAB account to Customer 1's DAB account at Crown Melbourne: SMR dated 31 July 2019.

Unusual transactions and patterns of transactions from August 2019 to November 2019

In August 2019, Customer 1 informed Crown that the Suncity junket would be closing its dedicated room at Crown Melbourne and transitioning towards running junkets on a casual basis only.

From this date, unusual transactional activity on Customer 1's DAB account continued but decreased in comparison to the level of activity in the preceding years.

On 21 September 2019, a telegraphic transfer of $20,000 from a third party, who was not noted as a key player under any Suncity junket programs, was deposited into Customer 1's DAB account at Crown Melbourne: SMR dated 23 September 2019.

On 12 November 2019, two telegraphic transfers of $100,000 from a third party, Person 30, who was not noted as a key player under any Suncity junket programs, were deposited into Customer 1's DAB account at Crown Melbourne: SMR dated 13 November 2019.

On 20 November 2019, a telegraphic transfer of $100,000 from a third party who was not noted as a key player under any Suncity junket programs, was deposited into Customer 1's DAB account at Crown Melbourne: SMR dated 21 November 2019.

On 13 December 2019, a set of three telegraphic transfers from three different bank accounts totalling $500,000 from a third party who was not noted as a key player under any Suncity junket programs, were deposited into Customer 1's DAB account at Crown Melbourne: SMR dated 16 December 2019.

In December 2019, eight telegraphic transfers of $100,000 each, and totalling $800,000, from a third party, Customer 20, a former key player not noted on any recent Suncity junket programs, were deposited into Customer 1's DAB account at Crown Melbourne: SMR dated 27 December 2019, 1 January 2020, and 2 January 2020.

2020

On 2 January 2020, a telegraphic transfer of $100,000 from a third party, Customer 20, was deposited into Customer 1's DAB account at Crown Melbourne: SMR dated 3 January 2020. Crown records show that Customer 20 had made telegraphic transfers totalling approximately $1,000,000 to Customer 1 in the previous two weeks.

On 22 March 2020, $241,000 was transferred from Customer 1's Crown Perth DAB account to another Crown patron, who was a personal assistant to a key player on the Suncity junket (who had refused to open a Crown Perth DAB account and claimed he had no bank account due to his celebrity status). The patron subsequently withdrew the full amount, which corresponded to the key player's winnings under the junket program, in cash: SMR dated 24 March 2020.

From March 2020, Customer 1 owed AUD$14,116,047 and HKD14,706,860 to Crown Melbourne.

Following the closure of the 2020 junket programs, Customer 1 left $1,337,169 in his safekeeping account. The funds were still parked in the account as at 18 June 2021. There had been no activity on the safekeeping account since 14 January 2021.

On 4 November 2020, Crown Melbourne received a telegraphic transfer of $1,233,600 from another Australian casino to a Crown Melbourne bank account on behalf of Customer 1, for the part repayment of a debt owed to Crown by Customer 1, but Crown was unable to verify the source of the funds prior to the transfer to Crown and notified the Australian bank to return the funds to the Australian casino: SMR dated 27 November 2020. An independent auditor identified Customer 1's failure to attempt to redeposit this payment as indicative of ML/TF typologies in its report.

749. On and from 1 March 2016, on multiple occasions, the provision of designated services by Crown Melbourne to players and representatives connected with the Suncity junket,

facilitated by Customer 1, raised red flags reflective of higher ML/TF risks as a result of unusual transactions and patterns of transactions made by junket representatives or junket players on the Suncity junkets through the Suncity cash administration desk.

Particulars

See paragraph 529ff.

2016

On 14 December 2016, Customer 1's junket representative withdrew $1,400,000 in cash from the Suncity cash administration desk: SMR dated 15 December 2016.

Suncity cash administration desk transactions from October 2017

From October 2017 to December 2017, there was a significant escalation in the number of reported suspicious cash transactions at the Suncity cash administration desk in Crown Melbourne.

During this period, Customer 1's junket representatives, key players on the Suncity junkets (including Customer 20, and Customer 22), as well as other third parties, made cash deposits and withdrawals at the Suncity cash administration desk, without any associated gaming activity.

Shortly before 4 October 2017, an unnamed junket representative for Customer 1 requested that Crown Melbourne provide a second cash counting machine in the Suncity room as the junket was expecting a large amount of cash to be delivered to the room and needed another machine to assist with counting. When prompted by Crown Melbourne, the representative did not wish to give details of the expected cash. On 4 October 2017, the Suncity Group Manager walked through Crown Melbourne with a small trolley suitcase containing $485,000 cash and delivered it to two unknown males in the Suncity room: SMR dated 6 October 2017.

On 7 October 2017, a junket representative for Customer 1deposited $340,000 in cash into her DAB account at the Suncity cash administration desk, then subsequently withdrew it, claiming that a key player wished to verify the funds: SMR dated 9 October 2017.

On 14 October 2017, Suncity representatives divided $800,000 into 16 bundles of $50,000 in $50 notes, then placed the bundles in two plastic bags at the Suncity cash administration desk. Suncity representatives provided this cash to another junket operator's (Customer 4) junket representative who took the cash to the Cage for counting and verification. At the Cage, the funds were then deposited into Customer 1's Crown Melbourne DAB account, and transferred to Customer 4's DAB account (although it is not clear which representative instructed this to occur). However, Suncity representatives refused to sign any documentation authorising the transfer into Customer 4's DAB account. As a result, the initial deposit and transfer was voided, and the cash was subsequently directly

deposited into Customer 4's DAB account: SMR dated 16 October 2017.

On 20 October 2017, a key player on the Suncity junket deposited $180,000 in cash at the Suncity cash administration desk and left after the transaction was completed: SMR dated 23 October 2017.

On 9 November 2017, an unknown male presented a briefcase of $400,000 cash at the Suncity cash administration desk, was given a receipt and left immediately after the cash was presented. Shortly after, a different unknown male presented a backpack of $400,000 cash, was given a receipt and left immediately after the cash was presented: SMR dated 17 November 2017.

On 24 November 2017, the following transactions occurred at the Suncity cash administration desk:

- key player Customer 20 presented two shopping bags of approximately $300,000 in cash to exchange for gaming chips at the Suncity cash administration desk: SMR dated 24 November 2017; and
- an unknown female associated with key player Customer 20 deposited $20,000 in cash at the Suncity cash administration desk, but did not participate in any gaming: SMR dated 27 November 2017.

On 26 November 2017, an unknown female acquired $30,000 in cash from the Suncity cash administration desk, placed the cash in a recyclable bag and subsequently did not participate in any gaming.

On 28 November 2017, a key player on the Suncity junket program deposited $83,550 in cash at the Suncity cash administration desk: SMR dated 29 November 2017.

On 29 November 2017, a key player on the Suncity junket program, Person 28, withdrew $200,000 in gaming chips from the Suncity cash administration desk and started playing. After he started playing, a Suncity representative placed three small bundles of cash in amounts from $5,000 to $10,000 each in front of the key player, which remained in front of him until he stopped playing. The key player then subsequently presented $225,360 in gaming chips and the cash bundles on his table to the Suncity cash administration desk, obtained a receipt and departed.

On 30 November 2017, a key player on the Suncity junket program deposited $60,000 in cash at the Suncity cash administration desk, then departed without play: SMR dated 30 November 2017.

On 30 November 2017, a key player on the Suncity junket program, Person 28, deposited $130,000 in cash at the Suncity cash administration desk, and departed without taking gaming chips: SMR dated 30 November 2017.

On 1 December 2017, a key player on the Suncity junket program, Person 28, deposited $100,000 in two telegraphic transfers into his DAB account, then withdrew the funds in cash. The cash was then presented at the Suncity cash administration desk for deposit: SMR dated 4 December 2017.

On 1 December 2017, an unknown male reported to possibly be a key player on the Suncity junket, Customer 25, presented $400,000 in cash at the Suncity cash administration desk, then departed without gaming: SMR dated 4 December 2017.

On 3 December 2017, there was a transaction of $116,000 between a third party, Customer 22, and a key player on the Suncity junket, Person 28, in the Suncity room: SMR dated 4 December 2017.

On 7 December 2017, an unknown male, reported to possibly be a Suncity agent, Person 59, withdrew $7,000, then departed without gaming: SMRs dated 8 December 2017 and 13 December 2017.

On 14 December 2017, a key player on the Suncity junket deposited $40,000 in cash at the Suncity cash administration desk into his Suncity account, then withdrew $50,000 in cash at the same Suncity cash administration desk approximately one hour later: SMR dated 15 December 2017.

On 15 December 2017, a key player on the Suncity junket presented $300,000 in cash at the Suncity cash administration desk in exchange for chips: SMR dated 18 December 2017.

On 16 December 2017, an unknown male deposited $40,000 in cash at the Suncity cash administration desk, then departed without gaming: SMR dated 19 December 2017.

On 20 December 2017, an unknown female presented$500,000 in $50 notes at the Suncity cash administration desk to be deposited into her account.

On 21 December 2017, a key player on the Suncity junket Customer 20 exchanged $700,000 in cash for chips at the Suncity cash administration desk, then proceeded to play: SMR dated 22 December 2017.

On 22 December 2017, the following transactions took place:

- an unknown male withdrew a large amount of cash from the Suncity cash administration desk, then departed without gaming: SMR dated 22 December 2017; and
- a key player on the Suncity junket, Person 28, exchanged $90,000 in cash in a paper shopping bag for chips at the Suncity cash administration desk, then proceeded to play: SMR dated 22 December 2017.

On 27 December 2017, a third party delivered approximately $210,000 in cash in $50 notes to the Suncity cash administration

desk, then departed without gaming: SMR dated 28 December 2017 and 12 January 2018.

On 29 December 2017, Customer 22 presented $150,000 in cash at the Suncity cash administration desk, then departed without gaming: SMR dated 29 December 2017.

On 30 December 2017, Customer 22 and his associate, Person 28, took approximately $100,000 in cash from a carry bag, handed it to the Suncity cash administration desk staff member, and both signed a receipt. Customer 22 and Person 28 subsequently returned to the Suncity room and deposited approximately $30,000 in cash in a white A4 envelope, and Customer 22 signed a receipt. Both individuals left, then subsequently returned to the Suncity room and deposited a further $40,000 in cash in another white A4 envelope, and Customer 22 again signed a receipt. Both individuals left again, then subsequently returned to the Suncity room and withdrew approximately $100,000 in cash in a carry bag, and Customer 22 again signed a receipt. Customer 22 subsequently returned to the Suncity room and deposited $50,000 in cash: SMR dated 2 January 2018.

On 30 December 2017, an unknown male deposited $50,000 in cash at the Suncity cash administration desk, then departed without playing: SMR dated 2 January 2018.

On 31 December 2017, a key player on the Suncity junket deposited $30,000 in cash at the Suncity cash administration desk: SMR dated 2 January 2018.

Suncity cash administration desk transactions from 2018

From 1 January 2018 to 10 January 2018, the following incidents of suspicious cash transactions at the Suncity cash administration desk, involving Customer 1's key players (including Customer 22 and Customer 20) and other third parties making large cash deposits into Customer 1's DAB account without associated gaming activity, were reported:

On 1 January 2018, the following transactions occurred:

- between 08:10am and 11:30am, Customer 22 handed various bundles of cash to the Suncity cash administration desk totalling $495,000, including:
    - at 08:10am, $100,000 in cash in a Crown carry bag;
    - at 08:40am, $80,000 in cash in a Crown carry bag;
    - at 09:05, $60,000 in cash;
    - at 10:20, $60,000 in cash;
    - at 10:42, $85,000 in cash;
    - at 10:55, $50,000 in cash; and

- at 11:30am, $60,000 in cash: SMR dated 2 January 2018.

- a Crown patron deposited $30,000 in cash at the Suncity cash administration desk: SMR dated 2 January 2018; and

- a key player on the Suncity junket deposited $50,000 in cash at the Suncity cash administration desk, then a further $30,000 in cash on a second occasion: SMR dated 2 January 2018.

On 2 January 2018, an unknown female deposited $30,000 in cash at the Suncity cash administration desk: SMR dated 3 January 2018.

On 3 January 2018, a key player on the Suncity junket, Person 28, deposited $60,000 cash at the Suncity cash administration desk: SMR dated 3 January 2018.

On 5 January 2018, a key player on the Suncity junkets, Customer 20, deposited $500,000 in $50 notes at the Suncity cash administration desk, then gamed for a short period of time before depositing a further $800,000 in cash: SMR dated 9 January 2018.

On 7 January 2018, a Crown patron, who was not a key player under any Suncity junket programs, attended the Suncity cash administration desk and withdrew approximately $10,000 cash, the departed without gaming: SMR dated 8 January 2018.

Around 9 January 2018, Customer 22 requested that Person 50, a junket representative, of another junket operator (Customer 2) obtain $200,000 worth of gaming chips from the Suncity cash administration desk, in circumstances where Customer 22 had no connection to the representative or his junket: SMR dated 9 January 2018.

On 10 January 2018, a key player on the Suncity junket program, Customer 20, presented a black suitcase of $155,000 cash at the Suncity cash administration desk: SMR dated 11 January 2018.

On 12 January 2018, a key player on the Suncity junket, Customer 23, deposited $100,000 in cash at the Suncity cash administration desk: SMR dated 15 January 2018.

On 13 January 2018, an unknown male, who had previously been sighted with key player, Customer 25, exchanged approximately $90,000 in cash for chips at the Suncity cash administration desk: SMR dated 16 January 2018.

On 14 January 2018, following a game in the Suncity room between a key player on the Suncity junket Person 47, Customer 26 and Customer 22, an undisclosed amount of gaming chips was deposited at the Suncity cash administration desk. Customer 26 subsequently withdrew $350,000 in cash from the Suncity cash administration desk, departed and handed the bag of cash to Customer 22 in the lift lobby: SMR dated 15 January 2018.

On 16 January 2018, a key player on the Suncity junket Customer 20 presented at the Suncity cash administration desk with $120,000 in cash to be used as buy-in for gaming.

On 19 January 2018, an unknown male deposited $20,000 in cash at the Suncity cash administration desk, then departed: SMR dated 23 January 2018.

On 24 January 2018, an unknown male, on behalf of two patrons, deposited $980,000 in cash in $50 notes, then subsequently departed without playing: SMRs dated 25 January 2018 and 31 January 2018.

On 25 January 2018, a key player on the Suncity junket, Customer 23, presented $130,000 in cash at the Suncity cash administration desk. The key player then won $52,000 in chips, but deposited the chips at the Suncity cash administration desk without obtaining cash in return: SMR dated 29 January 2018.

On 25 January 2018, a third party deposited $40,000 in cash at the Suncity cash administration desk.

On 31 January 2018, a key player on the Suncity junket, Customer 23, deposited $150,000 at the Suncity cash administration desk to exchange for chips.

On 8 February 2018, a key player on the Suncity junket Customer 20, presented $800,000 in cash in a paper bag covered by a black t-shirt at the Suncity cash administration desk and deposited $400,000 in cash, signed a receipt, and departed with the remaining $400,000 cash: SMR dated 9 February 2018.

On 13 February 2018, the following transactions occurred at the Suncity cash administration desk:

- a former key player on the Suncity junket deposited $300,000 in $50 notes contained in a backpack at the Suncity cash administration desk: SMR dated 15 February 2018; and
- an unknown male deposited $200,000 in cash (in $100 and $50 notes) at the Suncity cash administration desk: SMR dated 16 February 2018.

On 19 February 2018, a key player on the Suncity junket approached the Cage accompanied by Suncity staff members with $1,000,000 in cash in $50 notes. The cash was deposited into the key player's Crown Melbourne DAB account, and the funds were then telegraphic transferred to his Crown Perth DAB account: SMR dated 20 February 2018.

On 20 February 2018, a key player on the Suncity junket, Customer 25, deposited $250,000 in cash presented in $100 notes at the Suncity cash administration desk without any chips given in return: SMR dated 21 February 2018.

On 24 February 2018, a Crown patron deposited $338,050 and $288,400 in cash at the Suncity cash administration desk, removing the funds from a shoe box, then later attempted to exchange four counterfeit $100 notes at a Crown Melbourne table: SMR dated 27 February 2018.

On 25 February 2018, $700,000 in cash was withdrawn from Customer 1's Crown Melbourne DAB account. Shortly afterwards, Customer 1's junket representative subsequently presented two bags of $700,000 cash (in bundles of $10,000 in $100 notes) at the Suncity cash administration desk. Around this time, a key player on the Suncity junket arrived to play under the junket but waited until these funds were counted before commencing. Crown Melbourne was not aware of whetherf the cash was the same as that which had been withdrawn or if the funds belonged to the key player: SMR dated 26 February 2018.

On 26 February 2018, the following transactions occurred at the Suncity cash administration desk:

- Customer 1's junket representative, in the presence of a key player on the Suncity junket, Customer 25, presented a backpack of $100,000 in cash (in bundles of $10,000 in $100 notes) at the Suncity cash administration desk: SMR dated 26 February 2018; and
- a key player on the Suncity junket withdrew $480,000 and $470,000, totalling $950,000, in cash from the Suncity cash administration desk, then placed the cash into two blue cooler bags and departed: SMR dated 27 February 2018.

On 5 March 2018, an unknown male handed cash to the Suncity staff at the Suncity cash administration desk. Staff used the money counter to count $150,000 into 15 bundles of $10,000, which was taken back by the patron. Shortly afterwards, the same unknown male re-entered the Suncity room with a black suitcase of $50 notes, which was counted by Suncity staff, totalling $689,700, and divided into bundles of $150,000 placed into different shopping bags. The bags were then taken to the VIP lift lobby outside the Suncity room and given to a family which divided the bags between themselves.

On 7 March 2018, Customer 1's junket representative withdrew $1,910,000 in cash from Customer 1's Crown Melbourne DAB account, on behalf of a key player on the Suncity junket Customer 20, who said he "wished to take his funds in cash rather than sending funds out via telegraphic transfer": SMR dated 8 March 2018.

On 9 March 2018, a Crown patron deposited $230,000 in cash in $50 and $20 notes at the Suncity cash administration desk, but did not have an account with Suncity: SMR dated 9 March 2018.

On 13 March 2018, a key player on the Suncity junket, Customer 23, deposited $100,000 at the Suncity cash administration desk.

On 15 March 2018, a Crown patron (Person 11) who was not a key player under any Suncity junket programs, deposited $280,000 in cash in a paper shopping bag, then departed shortly afterwards: SMR dated 16 March 2018 and 21 March 2018.

On 16 March 2018, a key player on the Suncity junket deposited $1,009,840 in cash at the Suncity cash administration desk: SMR dated 19 March 2018.

On 19 March 2018, a Crown patron who was not noted as a key player under the Suncity junket programs, presented $80,000 in cash at the Suncity cash administration desk, then departed shortly afterwards: SMR dated 21 March 2018.

On 29 March 2018, Customer 1's junket representative deposited $1,500,000 in gaming chips at the Crown Melbourne Cage, an equivalent amount of which was subsequently withdrawn in cash at the Suncity cash administration desk: SMR dated 29 March 2018.

On 30 March 2018, a key player on the Suncity junket, Customer 23, deposited approximately $100,000 in cash at the Suncity cash administration desk, but left without gaming: SMR dated 3 April 2018.

On 6 April 2018, a key player on the Suncity junket deposited $50,000 cash at the Suncity cash administration desk, but was initially not forthcoming about his identity and departed shortly thereafter without play: SMR dated 6 April 2018.

On 15 April 2018, the following transactions occurred at the Suncity cash administration desk:

- two Crown patrons who played under the Meg-Star junket deposited $34,000 in cash (in $100 notes) at the Suncity cash administration desk, but the funds were returned when Meg-Star junket representatives refused to transfer the patrons to the Suncity junket: SMR dated 16 April 2018;
- a key player on the Suncity junket exchanged $34,000 cash for gaming chips at the Suncity cash administration desk: SMR dated 16 April 2018; and
- a key player on the Suncity junket deposited $39,000 cash at the Suncity cash administration desk: SMR dated 16 April 2018.

On 16 April 2018, a key player on the Suncity junket exchanged $90,000 in cash for gaming chips at the Suncity cash administration desk, then commenced gaming: SMR dated 17 April 2018.

April 2018 cash discovery at the Suncity cash administration desk (Crown Melbourne)

On 20 April 2018, Crown staff attended Pit 86 and the Suncity cash administration desk and located approximately $5,300,000 in cash at the Suncity cash administration desk and an additional $300,000 in cash located in cupboards. Later that day, Customer 1's junket representative presented $5,668,345 in cash at the Cage, divided between many different kinds of notes, counted and wrapped in plastic. This appeared to be the cash discovered by Crown staff following inspection of Pit 86 and the Suncity cash administration desk earlier that day.

750. On and from May 2017, Customer 1's junket representatives transacted on the Suncity Account on multiple occasions and Crown Melbourne failed to consider the ML/TF risks associated with providing designated services associated with this channel, before this channel was adopted.

Particulars

See paragraphs 423 and 513 to 515.

2017 Suncity Account transactions

In early May 2017, Crown reached an agreement to open an account with Suncity, for the purpose of receiving funds from key players who owed debts to Crown arising from junket program losses, which could be deposited at Suncity cash administration desks located in overseas casinos. By 25 September 2017, the Suncity Account held approximately HKD233,000,000 in deposited cash funds, on behalf of at least ten different Crown patrons, including Customer 27 and Customer 28.

May 2018 Suncity Account offset transaction

In April 2018, Crown Melbourne agreed to an arrangement with Customer 27 who owed approximately AUD$9,600,000 to Crown Melbourne. The agreement was that HKD28,684,094 in funds deposited into the Suncity Account at a Suncity cash administration desk by an agent of Customer 27 without notice to Crown in June 2017 (not credited to Crown Melbourne as the Suncity Account had been terminated), would be offset against 'lucky money' owed by Crown Melbourne to Customer 1. On 1 May 2018, Customer 1 executed an authority that directed the 'lucky money' funds be transferred to Customer 1's account with Suncity, which was effected. Crown Melbourne recorded in SYCO that Customer 27's debt to Crown Melbourne had been discharged and Crown Melbourne's debt to Customer 1 had also been discharged.

751. On and from 1 March 2016, on multiple occasions, action by law enforcement agencies in relation to matters connected to Customer 1, or the Suncity junket, junket representatives and key players associated with the Suncity junkets, raised red flags reflective of higher ML/TF risks for the provision of designated services to Customer 1 at Crown Melbourne and Crown Perth.

Particulars

On 16 November 2016, an enquiry was made by law enforcement in relation to Customer 1.

On 10 January 2018, Crown received a request for information from a law enforcement agency seeking footage of deposits made on 5 January 2018 by Customer 20 at the Suncity cash administration desk, who the law enforcement agency believed was accompanied by Customer 1.

On 25 February 2018, Crown received a request for information from law enforcement regarding a cash withdrawal of $700,000 at the Suncity cash administration desk.

On 20 April 2018, Crown received a request for information from law enforcement regarding a cash deposit of $5,600,000 on 20 April 2018 at the Suncity cash administration desk.

On 30 April 2018, Crown received a request for evidence from law enforcement in relation to transactions of $64,403 reported by a TTR and $39,000 reported by an SMR.

In December 2018, there were two suspicious cash transactions associated with the Suncity cash administration desk, the second leading to the arrest of a key player under the Suncity junket, Customer 23, by law enforcement:

- on 15 December 2018, an unknown male approached the Suncity cash administration desk and received three bundles of $50 notes (in a stack 10cm high), as well as 10 loose $100 notes, placed in a Crown cardboard bag, then departed the room: SMR dated 17 December 2018; and
- on 20 December 2018, Customer 23 and another person were arrested by a law enforcement agency after being located attempting to deposit $250,000 cash into a flagged Australian bank account. They had been given the money in a backpack in the valet parking area of Crown Melbourne by a Suncity junket representative who had retrieved the money from behind a curtain in the Suncity room inside Crown Melbourne: SMRs dated 21 December 2018 and 15 January 2019.

752. On and from 1 March 2016, the provision of designated services by Crown Melbourne and Crown Perth to Customer 1 posed higher ML/TF risks in circumstances where Crown Melbourne and Crown Perth were aware of publicly available information in relation to Customer 1.

Particulars

Allegations regarding Customer 1's involvement in receiving stolen funds

On 1 September 2017, Crown's Chief Legal Officer was notified by employees of Crown Aspinalls of Customer 1's alleged links to USD$81,000,000 in funds stolen from a central bank. Crown staff summarised the allegations from open source searches as follows:

- stolen money from the central bank was transferred to five fake bank accounts at another bank, then withdrawn and deposited into another account;
- the stolen money was subsequently withdrawn, converted into pesos by a remittance firm, and delivered to another individual; and

- the money was then deposited into casinos, by other individuals, including 903.73 million pesos deposited into Customer 1's account in an overseas casino.

Media allegations regarding Customer 1 in July 2019 – August 2019

From 27 July 2019 and August 2019, Crown Melbourne and Crown Perth were aware of media reports alleging that Customer 1 was:

- the subject of overseas law enforcement enquiries for engaging in illegal gambling;
- linked to organised crime;
- banned from entering Australia; and
- linked to money laundering through Australian casinos.

By at least 2 August 2019, Crown Melbourne and Crown Perth were aware of media reports alleging that Customer 1 had been denied a visa to enter Australia.

January 2020

On 2 January 2020, Crown Melbourne obtained an article alleging that Customer 1 and his Suncity junket had steered junket players to online and proxy betting and used underground banking for settlements.

February 2021 – Bergin Report

The Bergin Report found that it was "probable" that Customer 1 had a former association with organised crime and continued to associate with members of organised crime groups, and that there were links between Customer 1, the Suncity junket and organised crime groups. In addition, the Bergin Report found that the fact that large volumes of cash were being transacted in the Suncity room at the same time as media reports that Customer 1 was linked to organised crime should have alerted Crown to the "obvious and urgent" need to terminate its relationship with Customer 1 and his junket.

April 2021 – VCGLR Show Cause Decision

On 2 October 2020, the VCLGR issued a show cause notice issued with respect to Customer 1, alleging that Crown Melbourne had failed to have regard to matters involving Customer 1 and his Suncity junket, including Customer 1's connections to organised crime, large cash transactions involving Customer 1 and Suncity, and Suncity's non-compliance with cash controls imposed by Crown Melbourne. The show cause notice also referred to other individuals, including Customer 2, Customer 26 and Customer 32. On 27 April 2021, the VCGLR concluded that Crown Melbourne had breached section 121(4) of the *Casino Control Act* and imposed the maximum fine of $1,000,000.

November 2021 – Customer 1 arrested

On 27 November 2021, a law enforcement agency in a foreign country issued an arrest warrant for Customer 1. On 28 November 2021, Customer 1 was arrested by another foreign law enforcement agency and remanded on charges of alleged criminal association, illegal gambling, money laundering and running an illegal online gambling operation in a foreign country.

753. At no time did Crown Melbourne or Crown Perth undertake appropriate risk-based customer due diligence with respect to Customer 1 with a view to identifying, mitigating and managing the ML/TF risks posed by the provision of designated services on and from 1 March 2016.

a. Crown Melbourne was aware of unusual and suspicious transactional activity with respect to Customer 1, including from late 2017, cash deposits by third parties and other transactions consistent with ML/TF typologies.

b. Crown Perth was aware of unusual and suspicious transactional activity with respect to Customer 1 and key players on his junkets and other transactions consistent with ML/TF typologies.

c. At no time did Crown Melbourne or Crown Perth take appropriate steps to understand whether Customer 1's source of wealth/funds was legitimate.

d. At no time did Crown Melbourne or Crown Perth take appropriate steps to identify or analyse the ML/TF risks of Customer 1's transactions or to consider whether they had a lawful purpose.

e. With the exception of returning payments made by Customer 1's company on 6 June 2012 and 25 February 2013, $693,000 sent by a third party marked as "payment to supplier" on 24 May 2019, and $1,233,600 sent by another Australian casino on 4 November 2020, Crown Melbourne or Crown Perth gave no consideration to whether large and high risk transactions should be processed.

f. On each occasion prior to January 2021 that senior management considered whether to continue the business relationship with Customer 1, senior management failed to give adequate consideration to whether the ML/TF risks posed by Customer 1 were within Crown Melbourne and Crown Perth's risk appetite.

Particulars

Section 36(1)(a) of the Act.

Database searches

Between 2017 and 2019, the Credit control team performed property searches and company searches on Customer 1.

Between 25 July 2019 and 1 August 2019, Crown AML employees performed company searches, Australian company searches, property title searches, media report searches, and risk intelligence searches. Crown AML employees also obtained wealth reports, and articles from open source searches, apparently for the purpose of responding to the media allegations.

By 29 July 2019, Crown had obtained media reports that alleged that Crown engaged in business with junket operators, including Customer 1, who were backed by organised crime syndicates.

On 2 August 2019, Crown Resorts obtained articles alleging that Customer 1 had been banned from entering Australia at the same time as investigations were conducted into his links to organised crime. The articles were provided to the Chief Legal Officer.

On 10 August 2019, Crown obtained articles alleging that Customer 1 was linked to money laundering transactions at another Australian casino, including a cash deposit of $403,000.

Over the course of 2020, Crown performed a number of database and open source searches in connection with Customer 1.

Junket profile

In early 2017, the Credit control team drafted a junket profile on Customer 1, which summarised:

- findings of wealth reports, which recorded that Customer 1 was allegedly a former organised crime member in charge of loan sharking and gambling;
- findings of risk intelligence reports, which identified Customer 1 as a foreign PEP and that media reports stated that Customer 1 is affiliated with individuals involved in organised crime; and
- open source searches, which included reference to Customer 1's alleged receipt of funds stolen from a central bank.

On 25 May 2017, July 2018, 19 March 2019, 14 August 2019, and 1 September 2020, Customer 1's junket profile was updated. Each iteration of the profile recommended that Crown continue to conduct business with Customer 1, but did not provide a basis for this recommendation.

By 14 January 2021, Customer 1's updated junket profile noted that Customer 1 owed AUD$14,116,047 and HKD14,706,860 to Crown Melbourne, and noted under the heading 'AML Check' that 250+ SMRs had been given to the AUSTRAC CEO and five law enforcement enquiries made with respect to Customer 1 between 2016 and 2020.

Senior management engagement in 2017

On 4 January 2017, Customer 1's junket profile was circulated to Senior Vice President (International Business), Chief Executive Officer (Australian Resorts), Chief Executive Officer (Crown Resorts), Crown Resorts director, General Counsel, (Crown Resorts), Executive General Manager (Legal and Regulatory Services), and Group General Manager (International Business Operations) to be discussed at a meeting of the VIP Committee.

On 25 May 2017, Customer 1's junket profile was provided to the Chief Legal Officer, along with supporting documents referred in the profile.

Approval to continue relationship with Customer 1 after identification as a foreign PEP (Crown Melbourne only)

On 5 June 2017, the CTRM identified that Customer 1 was a foreign PEP and requested approval from the Chief Legal Officer for Crown to continue a business relationship with Customer 1.

On 16 June 2017, Crown's Chief Legal Officer granted approval for Crown Melbourne to continue its relationship with Customer 1, without recording any reasons in writing.

On 28 July 2017, the Crown Perth AML/CTF Compliance Officer determined to increase Customer 1's risk rating to High, without recording any reasons in writing.

On 1 September 2017, Crown's Chief Legal Officer was notified of media articles reporting Customer 1's alleged links to USD$81,000,000 in funds stolen from a central bank, which had been deposited into a Suncity account in an overseas casino.

On 6 September 2017, Crown's Chief Legal Officer considered whether Crown Resorts, including Crown Aspinalls, should proceed with doing business with Customer 1 in light of the above media articles. An employee from Crown Aspinalls advised the Chief Legal Officer that a Crown Aspinalls senior manager had spoken to Customer 1 who stated that the funds had been deposited by one of the many agents working for Customer 1.

The Chief Legal Officer escalated the matter to the Chief Executive Officer (Australian Resorts) who confirmed that Crown was comfortable continuing to do business with Customer 1.

Senior management engagement in 2018

In March 2018, a large amount of cash was discovered in the Suncity room. On 24 March 2018, the Group General Manager (International Business Operations) sent a Crown employee an email asking him to inform Suncity senior staff that cash transactions at the Suncity cash administration desk and Pit 86 were no longer permitted and cash held at the desk should not exceed $100,000 for non-gaming uses.

On 17 April 2018, Crown advised Suncity staff again regarding the additional cash controls, to take effect on 20 April 2018.

On 20 April 2018, Crown staff attended Pit 86 and the Suncity cash administration desk and located $5,300,000 at the Suncity cash administration desk and an additional $300,000 located in cupboards.

On 20 April 2018, the Chief Legal Officer and Group General Manager – AML, met to discuss, among other things, Customer 1 and the Suncity junket. The Group General Manager – AML advised the Chief Legal Officer of her concerns regarding Suncity. An action item

from the meeting included to review the volume and value of Suncity SMRs given to the AUSTRAC CEO by Crown Melbourne.

'ML/TF assessment' by the Group General Manager – AML

On 16 May 2018, the Senior Vice President (International Business) prepared a note on the Suncity junket business which stated that bank transfers in relation to the Suncity junket to and from Customer 1, junket players, third parties and Customer 1's foreign junket company, and cash transactions are common as they are winnings from another casino, cash is convenient and private, and there was a preference to take winnings as cash to use as buy-in for the next trip.

On 23 May 2018, Group General Manager AML prepared a document titled 'ML/TF Risk Assessment' for Customer 1. The document:

- noted that Crown Melbourne was aware of media allegations regarding Customer 1's organised crime links but stated that Customer 1 had not been charged with an offence;
- described the risks of cash transactions occurring at the Suncity cash administration desk in Pit 86 and described existing and enhanced controls in relation to this risk, but did not identify any other ML/TF risks; and
- stated that following the review and implementation of controls, Crown Melbourne had determined that it remained appropriate to continue to do business with Customer 1, his junket representatives and key players.

The document did not adequately identify or address the ML/TF risks posed by Customer 1, including the high turnover of his junkets, the non-cash transactions by third parties on his DAB account and patterns of transactions indicative of ML/TF risks: see paragraph 534 and 535.

July 2019 – August 2019 media allegations

On 18 July 2019, Crown's AML team obtained media articles alleging that Suncity was under scrutiny by authorities for engaging in online gaming and proxy betting operations, but that gaming regulator inspections had uncovered nothing illegal, which were noted on Crown Melbourne's risk history for Customer 1.

On 23 July 2019, Crown Resorts received a media enquiry from Australian media which alleged that Customer 1 was connected to organised crime.

On 29 July 2019, the Chief Legal Officer prepared a draft Board Paper regarding the Australian broadcast program that noted the adverse entries against Customer 1 in wealth reports and law enforcement enquiries related to Customer 1.

Around 11 and 12 August 2019, Suncity informed Crown that it would be winding back operations, removing the dedicated room and staff, and running the junket as a casual junket only.

On 16 August 2019, Crown Resorts received a second media enquiry in relation to Customer 1, which queried whether Crown had taken any action to examine its links to Customer 1's Suncity business or close its Suncity room.

On 20 August 2019, the Chief Legal Officer prepared an updated memorandum to the Board of Crown Resorts, which outlined that the Suncity junket's turnover at Crown Melbourne and Crown Perth to July 2019 was $28,692,442,000, set out background information on Customer 1, including the findings from wealth reports, law enforcement enquiries, and risk intelligence and media report searches, noted that Crown senior managers overseas were unaware of media allegations of links to organised crime and noted that Suncity had informed Crown it would be closing the Suncity room and running the junket on a casual basis.

Senior management engagement in 2020

On 10 June 2020, the Chief Legal Officer wrote to the Chief Executive Officer (Australian Resorts) and Chief Executive Officer (Crown Resorts) providing an update to earlier emails sent in March 2020 regarding Customer 1 and another junket operator, Customer 2. The email referred to the development of proposed junket controls for Customer 1 which will be implemented in advance of recommencing international business following the COVID-19 shutdown.

On 12 September 2020, Crown obtained an external due diligence report in relation to Customer 1, which noted the following key issues:

- Customer 1's alleged organised crime background was not uncommon as it was beneficial for both the junket operator and organised crime;
- Customer 1 was linked to the receipt of stolen funds from a central bank in April 2016, but was not the focus of proceedings or follow-up litigation in foreign courts;
- Customer 1 was involved in online gambling portals in 2019, through broadcasting of overseas games to Suncity client computers or phone screens;
- sources alleged Customer 1 had engaged in money-laundering for foreign government officials and business people;
- Customer 1's acquisition of listed companies was suspect, with sources suggesting that Customer 1 had obtained controlling interests in listed companies through his association with a syndicate; the syndicate supplied loans to gamblers who owned listed companies and would use the companies as collateral;

failure to repay the loans would lead to the syndicate taking over the listed companies via proxies; and

- sources alleged prior to more recent real estate development projects, Customer 1's companies did not have active legitimate business operations but were in fact connected to money laundering and junkets.

On 11 November 2020, Crown prepared a document which reviewed wealth reports identifying links between Customer 1 and another junket operator, Customer 3, who ran the Meg-Star junket.

By November 2020, Crown had applied stop codes against Customer 1, but had not issued a WOL.

On 20 January 2021, the Crown Resorts POI Committee considered Customer 1, who had come to the Committee's attention through the ILGA inquiry. The Committee agreed to apply a WOL against Customer 1.

On 22 January 2021, the WOL took effect at Crown Melbourne.

On 29 January 2021, the NRL took effect at Crown Perth.

Prior to January 2021, none of these steps were proportionate to the ML/TF risks reasonably posed by Customer 1.

Enhanced customer due diligence

754. On and from 1 March 2016, Crown Melbourne gave the AUSTRAC CEO an SMR with respect to Customer 1 on the occasions outlined in Schedule 3.1.

Particulars

The SMRs reported:

- annual losses by key players on the Suncity junkets;
- Customer 1's telegraphic transfers with third parties; and
- large cash deposits into and withdrawals from Customer 1's DAB account.

755. On each occasion that Crown Melbourne formed a suspicion with respect to Customer 1 for the purposes of s41 of the Act, it should have conducted ECDD.

Particulars

Rule 15.9(3) of the Rules.

756. Crown Melbourne did not carry out appropriate risk-based ECDD measures with respect to Customer 1 on each occasion that Crown Melbourne formed a suspicion with respect to Customer 1 for the purposes of s41 of the Act.

a. With the exception of the SMRs given to the AUSTRAC CEO in January 2020, there are no records of ECDD being conducted following the lodgement of the SMRs between 1 March 2016 and 27 November 2020. To the extent that some due diligence was performed by the Credit control team in the period following the lodgement of the SMR, it was not adequate or appropriate: see paragraphs 664 and 685.

b. Appropriate risk-based steps were not taken to obtain or analyse information about Customer 1's source of wealth/funds: see paragraph 667.

c. Appropriate risk-based steps were not taken to analyse and monitor Customer 1's transactions – both past and future – including to understand their economic purpose: see paragraphs 590 and 666.

d. On each occasion prior to January 2021 that senior management considered whether to continue the business relationship with Customer 1, senior management failed to give adequate consideration to whether the ML/TF risks posed by Customer 1 were within Crown Melbourne's risk appetite: see paragraph 668ff.

Particulars

Rule 15.9(3), rule 15.10(1)(c), (d), (2), (5) and (6) of the Rules.

See particulars to paragraph 753.

757. On and from 1 March 2016, Crown Perth gave the AUSTRAC CEO an SMR with respect to Customer 1 on the occasions outlined in Schedule 3.1.

Particulars

The SMRs described:

- Customer 1's telegraphic transfers with third parties; and
- suspicions raised with respect to activities by key players on the Suncity junkets.

758. On each occasion that Crown Perth formed a suspicion with respect to Customer 1 for the purposes of s41 of the Act, it should have conducted ECDD.

Particulars

Rule 15.9(3) of the Rules.

759. Crown Perth did not carry out appropriate risk-based ECDD measures with respect to Customer 1 on each occasion that Crown Perth formed a suspicion with respect to Customer 1 for the purposes of s41 of the Act.

a. There are no records of ECDD being conducted following the lodgement of the SMRs between 23 February 2019 and 24 March 2020. To the extent that some due diligence was performed by the Credit control team in the period following the lodgement of an SMR, it was not adequate or appropriate: see paragraphs 664 and 685.

b. Appropriate risk-based steps were not taken to obtain or analyse information about Customer 1's source of wealth/funds: see paragraph 667.

c. Appropriate risk-based steps were not taken to analyse and monitor Customer 1's transactions – both past and future – including to understand their economic purpose: see paragraphs 590 and 666.

d. On each occasion prior to January 2021 that senior management considered whether to continue the business relationship with Customer 1, senior management failed to give adequate consideration to whether the ML/TF risks posed by Customer 1 were within Crown Perth's risk appetite: see paragraph 668ff.

Particulars

Rule 15.9(3), rule 15.10(1)(c), (d), (2), (5) and (6) of the Rules.

See particulars to paragraph 753.

760. At all times from 1 March 2016, Customer 1 was a foreign PEP.

Particulars

Section 36(1)(a)

See particulars to paragraph 738.

761. At all times from 1 March 2016, Crown Melbourne and Crown Perth were required to apply their ECDD program to Customer 1.

Particulars

Rule 15.9(2) 15.11 of the Rules.

See paragraphs 660, 663 and 666.

762. Crown Melbourne did not carry out appropriate risk-based ECDD measures with respect to Customer 1 on and from 1 March 2016 given his status as a foreign PEP. In particular:

a. Crown Melbourne did not undertake a detailed analysis of Customer 1's KYC information or analyse the legitimacy of Customer 1's source of wealth/funds.

b. On occasions where senior management approved a continuing business relationship with Customer 1 as a foreign PEP, the decision did not have adequate regard to the ML/TF risks posed by Customer 1.

c. On occasions where senior management approved continuing to provide designated services to Customer 1 as a foreign PEP, the decision did not have adequate regard to the ML/TF risks posed by Customer 1.

Particulars

Rule 15.10(2), 15.10(6), 15.11 of the Rules.

See particulars to paragraph 753.

See paragraph 660, 663, 666, 667 and 668.

763. Crown Perth did not carry out appropriate risk-based ECDD measures with respect to Customer 1 on and from 1 March 2016 given his status as a foreign PEP. In particular:

a. Crown Perth did not undertake a detailed analysis of Customer 1's KYC information or analyse the legitimacy of Customer 1's source of wealth/funds;

b. On occasions where senior management approved a continuing business relationship with Customer 1 as a foreign PEP, the decision did not have adequate regard to the ML/TF risks posed by Customer 1.

c. On occasions where senior management approved continuing to provide designated services to Customer 1 as a foreign PEP, the decision did not have adequate regard to the ML/TF risks posed by Customer 1.

Particulars

Rule 15.10(2), 15.10(6) and 15.11 of the Rules.

See particulars to paragraph 753.

See paragraph 660, 663, 666, 667 and 668.

764. On and from 5 June 2017, Crown Melbourne rated Customer 1 high risk.

Particulars

Between 5 June 2017 and 12 October 2021, Crown Melbourne rated Customer 1 high risk on 162 occasions.

See particulars to paragraph 741.

765. On each occasion that Crown Melbourne rated Customer 1 high risk, Crown Melbourne was required to apply its ECDD program to Customer 1.

Particulars

Rule 15.9(1).

See paragraph 661.

766. Crown Melbourne did not carry out appropriate risk-based ECDD measures with respect to Customer 1 on each occasion that Crown Melbourne rated Customer 1 high risk.

Particulars

Despite the matters pleaded at paragraphs 737, 738, 746, 747, 748, 749, 750, 751, and 752, other than following submission of the SMRs in January 2020, at no time did Crown Melbourne conduct ECDD following each occasion that it rated Customer 1 high risk: see paragraph 753.

See paragraphs 661, 666, 667 and 668.

767. On and from 28 July 2017, Crown Perth rated Customer 1 high risk.

Particulars

Between 28 July 2017 and 23 March 2020, Crown Perth rated Customer 1 high risk on 5 occasions.

See particulars to paragraph 744.

768. On each occasion that Crown Perth rated Customer 1 high risk, Crown Perth was required to apply its ECDD program to Customer 1.

Particulars

Rule 15.9(1).

See paragraph 661.

769. Crown Perth did not carry out appropriate risk-based ECDD measures with respect to Customer 1 on each occasion that Crown Perth rated Customer 1 high risk.

Particulars

Despite the matters pleaded at paragraphs 737, 738, 746, 747, 748, 751, and 752, at no time did Crown Perth conduct adequate ECDD following each occasion that it rated Customer 1 high risk: see paragraph 753.

See paragraphs 661, 666, 667 and 668.

770. By reason of the matters pleaded from paragraphs 731 to 769, on and from 1 March 2016, Crown Melbourne and Crown Perth:

a. did not monitor Customer 1 in relation to the provision of designated services, with a view to identifying, mitigating and managing the ML/TF risks reasonably faced; and

b. did not do so in accordance with rr15.5 and 15.9 of the Rules.

771. By reason of the matters pleaded at paragraph 770, Crown Melbourne and Crown Perth contravened s36(1) of the Act on and from 1 March 2016 to 22 January 2021 (Crown Melbourne) and 29 January 2021 (Crown Perth) with respect to Customer 1.

Particulars

Section 36(1) of the Act is a civil penalty provision: s36(2) of the Act.

Customer 2

772. Customer 2 was a customer of Crown Melbourne from 25 May 2009 to 22 January 2021.

773. From at least 24 July 2009, Crown Melbourne provided Customer 2 with designated services within the meaning of table 1 and table 3, s6 of the Act.

774. From at least 24 July 2009, Customer 2 received designated services as a junket operator and as a junket player, facilitated through his own junket program, at Crown Melbourne.

Particulars to paragraphs 773 and 774

On 25 May 2009, Crown Melbourne entered into a NONEGPRA with Customer 2 to operate junkets at Crown Melbourne. An updated NONEGPRA was entered into on 7 March 2019.

On 11 August 2009, Crown Melbourne opened a DAB account and safekeeping account for Customer 2.

On 24 July 2009, Crown Melbourne approved a credit facility (AUD/HKD) for Customer 2, under Customer 2's first PID. On 24 November 2020, Crown Melbourne closed the credit facility.

On 24 May 2015, Crown Melbourne opened a second DAB account and safekeeping account for Customer 2 under a different PID.

On 11 November 2016, Crown Melbourne opened a third DAB account and safekeeping account for Customer 2 under a different PID.

Between 9 March 2016 and 23 March 2020, Customer 2 operated at least 68 junket programs at Crown Melbourne, including 40 under an initial PID, 26 under a second PID and 2 under a third PID. In that period, Customer 2 had approximately six junket representatives.

Customer 2 received designated services as a junket player under his own junket program.

On 22 January 2021, Crown Melbourne issued an indefinite WOL in respect of Customer 2.

775. Customer 2 was a customer of Crown Perth from 17 August 2009 to 29 January 2021.

776. From at least 17 August 2009, Crown Perth provided Customer 2 with designated services within the meaning of table 1 and table 3, s6 of the Act.

777. From at least 17 August 2009, Customer 2 received designated services as a junket operator and as a junket player, facilitated through his own junket program, at Crown Perth.

Particulars to paragraphs 776 and 777

On 17 August 2009, Crown Perth opened a DAB account and safekeeping account for Customer 2 under his only PID at Crown Perth.

On 17 August 2009, Crown Perth approved a FAF (AUD/HKD) for Customer 2 under the same PID as the above accounts.

On 20 October 2010, Crown Perth entered into a NONEGPRA with Customer 2 to operate junkets at Crown Perth. An updated NONEGPRA was entered into on 7 March 2019.

On 15 July 2011, Crown Perth made Customer 2 a premium program player.

Between 25 October 2017 and 12 August 2019, Customer 2 operated at least four junkets at Crown Perth under one PID. In that period, Customer 2 had approximately six junket representatives.

On 29 January 2021, Crown Perth issued an indefinite WOL against Customer 2.

Customer 2 received designated services as a junket player under his own junket program.

The ML/TF risks posed by Customer 2

778. By 1 March 2016, higher ML/TF risks were indicated by the nature and purpose of Customer 2's business relationship with Crown Melbourne and Crown Perth, the nature of the transactions he had been conducting, together with the suspicions Crown Melbourne itself had formed with respect to Customer 2.

Particulars

Section 36(1)(a), (b) of the Act and Chapter 15 of the Rules.

Customer 2 was a junket player and junket operator. He received designated services through the channel of junket programs. This channel lacked transparency: see paragraph 477.

Junket programs – Crown Melbourne

By 1 March 2016, Customer 2 had operated approximately 89 junket programs at Crown Melbourne. Crown Melbourne recorded that the total turnover for those programs was approximately $24,525,270,063, with losses of approximately $271,014,648.

Commissions of approximately $186,829,105 were payable by Crown Melbourne to Customer 2.

Junket programs – Crown Perth

By 1 March 2016, Customer 2 had operated approximately 19 junket programs at Crown Perth. Crown Perth recorded that the total turnover for those programs was approximately $163,152,650, with losses of approximately $12,332,790. Commissions of approximately $1,297,548 were payable by Crown Perth to Customer 2.

Credit facilities

By 1 March 2016, Crown management approved numerous credit facilities for Customer 2's junkets prior to the junket programs in various amounts as a standing credit line, with limits ranging from $1,000,000 in 2009, up to AUD$20,000,000 / HKD140,000,000 in 2016.

SMRs

By 1 March 2016, Crown Melbourne had given the AUSTRAC CEO 77 SMRs in relation to Customer 2.

The SMRs reported:

- suspicions relating to key player losses;
- key players on Customer 2's junkets claiming winnings where there was no or inconsistent rated gaming recorded for each player (totalling $1,146,600);
- cashing-in large value chips without betting;
- high volumes of telegraphic transfers into Customer 2's DAB account at Crown Melbourne from third parties;
- high volumes of telegraphic transfers withdrawn from Customer 2's DAB account at Crown Melbourne and sent to third parties;
- third party deposits to Customer 2's DAB account from Person 41 (see particulars to paragraphs 968 and 969), totalling $3,608,604 in less than a month;
- suspicious cash deposits and cheque deposits; and
- unusual transfers between Customer 2's DAB account and other Crown patrons.

Collectively, the SMRs given to the AUSTRAC CEO in relation to Customer 2 between 28 May 2010 and 26 September 2012 reported total wins of $9,208,035 and total losses of $20,884,110. The SMRs also reported total wins of $716,750 and total losses of $1,963,515 for Customer 2 in his capacity as a junket player. Customer 2 played on at least three junket programs during this period.

Suspicious transactions

By 1 March 2016, Crown Melbourne had identified a number of suspicious transactions involving Customer 2, including:

- on 25 May 2010, Customer 2 transferring $330,000 from his DAB account to a Crown patron's DAB account, who then on-transferred $310,000 to his wife's DAB account. His wife then exchanged $127,000 in gaming chips to cash;
- on 17 May 2011, Customer 2's junket representative, Person 54, approached the Cage with two cheques for $950,000 and $1,000,000, which were deposited into his DAB account, then transferred to Customer 2's DAB account: SMR dated 18 May 2011;
- on 1 March 2012, Customer 2's junket representative, Person 54, approached the Cage with three unidentified individuals, and deposited a suitcase of cash containing AUD$2,201,000 and foreign currency totalling AUD$1,327,610: SMR dated 2 March 2012;
- on 12 May 2012, $6,210,000 was transferred from Customer 2's DAB account to a Crown patron's DAB account, which was subsequently withdrawn and sent via telegraphic transfer to the Crown patron's Australian bank account: SMR dated 14 May 2012;
- on 20 March 2013, Customer 2's personal assistant deposited a bank cheque for $3,100,000 into his DAB account, then transferred the funds to Customer 2's DAB account: SMR dated 20 March 2013;
- on 29 April 2013, Customer 2's junket representative, Person 54, deposited $650,000 in $50 notes into Customer 2's DAB account, then withdrew them in cash chips, which was suspicious because the Customer 2 junket used commission-based chips, not cash chips: SMR dated 30 April 2013;
- on 3 December 2013, a Crown staff member approached the Cage with $200,000 in cash to deposit into Customer 2's DAB account, on behalf of Customer 2's junket representative, Person 26. Person 26 had completed a number of transactions through a Crown staff member which was suspicious as it appeared that he was avoiding completing the transactions himself: SMR dated 4 December 2013; and
- on 26 February 2014, $500,000 was transferred from Customer 2's DAB account to another Crown patron's DAB account: SMR dated 27 February 2014.

Other red flags

On 16 December 2012, $747,000 was withdrawn from Customer 2's DAB account and sent via telegraphic transfer to an automotive company: SMR dated 17 December 2012. In 2016, this transaction was the subject of proceeds of crime proceedings in an Australian

court, on the basis that the funds were used to purchase a car and the car was purchased using the proceeds of crime relating to money-laundering or tax avoidance.

On 19 July 2013, Customer 2 deposited $1,700,000 into his safekeeping account at Crown Melbourne and provided an authority to remit funds to Crown Aspinalls to secure the purchase of gaming chips by a junket representative at Aspinalls: see also paragraphs 332ff and 375ff.

A report by an independent auditor identified that in 2015 Customer 2 engaged in transactions indicative of ML/TF typologies involving quick turnover of funds (without betting), including on 16 December 2015, when he deposited $312,600 by telegraphic transfer, then withdrew $312,624 from his DAB account by telegraphic transfer on that same day.

Law enforcement enquiries

Between 7 May 2013 and 10 December 2015, law enforcement enquiries were made in respect of Customer 2 on ten separate occasions.

Third party deposits returned to depositor

On 7 January 2014, Crown Melbourne received a funds transfer of $1,200,000 from a third party company for the benefit of Customer 2. On 10 January 2014, Crown Melbourne arranged for the funds to be returned to the original depositor.

On 17 June 2014, Crown Melbourne received a funds transfer of $1,090,000 from a third party company for the benefit of Customer 2. On 17 June 2014, the funds were returned because Crown Melbourne had only received a letter authorising the deposit from one of two directors.

Due diligence

By 1 March 2016, the due diligence steps taken with respect to Customer 2 included the following.

As part of Customer 2's initial application for credit and subsequent re-approvals, Crown obtained information from overseas Crown staff about Customer 2's business activities in order to assess his creditworthiness, and was advised that Customer 2 was an established junket operator who operated junkets using credit facilities at overseas casinos, with an associate, Person 14.

At no time between 2010 and 2016, did Crown Melbourne or Crown Perth perform any other due diligence on Customer 2.

779. As at 1 March 2016, Customer 2 should have been recognised by Crown Melbourne as a high risk customer for the reasons pleaded at paragraph 778.

Particulars

Section 36(1)(a), (b) of the Act and Chapter 15 of the Rules.

780. At all times on and from 1 March 2016, Customer 2 should have been recognised by Crown Melbourne as a high risk customer by reason of the matters pleaded at paragraphs 778, 785, 786, 787, 788, 789, 790 and 792.

Particulars

Section 36(1)(a), (b) of the Act and Chapter 15 of the Rules.

781. It was not until 20 January 2021 that Customer 2 was rated high risk by Crown Melbourne.

Particulars

On approximately 108 occasions between 25 August 2009 and 30 April 2013, Crown Melbourne assessed Customer 2 as moderate risk.

On approximately 317 occasions between 7 May 2013 and 20 May 2020, Crown Melbourne assessed Customer 2 as significant risk.

See paragraph 481.

782. As at 1 March 2016, Customer 2 should have been recognised by Crown Perth as a high risk customer for the reasons pleaded at paragraph 778.

Particulars

Section 36(1)(a), (b) of the Act and Chapter 15 of the Rules.

783. At all times on and from 1 March 2016, Customer 2 should have been recognised by Crown Perth as a high risk customer by reason of the matters pleaded at paragraphs 778, 785, 786, 787, 788, 789 and 795.

Particulars

Section 36(1)(a), (b) of the Act and Chapter 15 of the Rules.

784. It was not until 20 January 2021 that Customer 2 was rated high risk by Crown Perth.

Particulars

There is no evidence that Crown Perth assessed Customer 2's risk rating at any time prior to 20 January 2021. The default risk rating of low applied.

See paragraph 481.

785. On and from 1 March 2016 designated services provided to Customer 2 posed higher ML/TF risks including because the provision of designated services to Customer 2 involved a combination of the following factors:

a. Customer 2 received high value financial (table 1, s6) and gaming services (table 3, s6) provided through multiple junket programs: see paragraph 473ff;

b. Customer 2 was a junket operator who facilitated the provision of high value financial and gaming services (tables 1 and 3, s6) to key players on his junket programs: see paragraph 473ff;

c. Customer 2 was the ultimate beneficial owner of his junket;

d. Customer 2 was a junket player;

e. by no later than March 2020, turnover for Customer 2's junket had exceeded approximately $10,561,102,323 at Crown Melbourne;

f. by no later than March 2020, turnover for Customer 2's junket had exceeded approximately $74,123,400 at Crown Perth;

g. Customer 2 was known at all times to be connected to other junket operators, including junket operators in respect of whom Crown Melbourne or Crown Perth had formed suspicions including Customer 1 and Customer 11;

h. designated services provided to Customer 2 lacked transparency as the services were provided through the channel of junket programs: see paragraph 477(e);

i. persons associated with Customer 2's junket transacted using large amounts of cash and cash that appeared suspicious, including large volumes of cash, primarily in $50 notes, wrapped in rubber bands or plastic: see paragraphs 450, 451, 452 and 491;

j. the table 3, s6, designated services provided to Customer 2 involved high turnover;

k. designated services provided to Customer 2 involved large transfers to and from third parties, including to and from other junket operators, foreign remittance service providers and unknown third parties: see paragraph 456ff;

l. designated services provided to Customer 2 involved large cross-border movements of funds, including through a Southbank account: see paragraph 239;

m. large values of funds were transferred to and from Customer 2's DAB account and other customers' DAB accounts, involving designated services within the meaning of items 31 and 32, table 1, s6 of the Act;

n. at various times, Customer 2 was provided with significant amounts of credit upon request, up to limits of $20,000,000, including a standing credit line which was reapproved on a regular basis until March 2020: see paragraphs 280ff and 487;

o. Customer 2 or his junket representatives engaged in other transactions indicative of ML/TF typologies and vulnerabilities, including structuring, cashing-in large value chips with no evidence of play, and quick turnover of funds (without betting): see paragraph 24;

p. in January 2018, Customer 2's junket representatives engaged in large cash transactions on behalf of third parties, including Customer 22;

q. Crown Melbourne made available the Crown private jet for Customer 2's junket. There were inadequate controls on the carrying of large amounts of cash on Crown's private jets*:* see paragraphs 454 and 491(c);

r. these transactions took place against the background of:

    i. law enforcement agencies made enquiries in relation to Customer 2 on 10 occasions between 7 May 2013 and 10 December 2015; and

    ii. 77 SMRs being given to the AUSTRAC CEO by Crown Melbourne by 1 March 2016.

s. in 2016 and 2017, Customer 2 was the subject of law enforcement enquiries on two occasions;

t. by December 2016, Crown Melbourne was aware of reports alleging that:

i. Customer 2 had been convicted and imprisoned in 2003 for illegal gambling activities;

ii. Customer 2's business associate had been the subject of orders to arrest for attempted bribery of government officials in a foreign jurisdiction; and

iii. funds sent from Customer 2's DAB account at Crown Melbourne used to purchase a luxury car were the subject of proceeds of crime proceedings in an Australian court in 2016, which related to allegations of suspected money laundering or and tax avoidance;

u. by August 2019, media reports named Customer 2 as a person involved in conducting junkets at Crown Melbourne, despite having been convicted and imprisoned in 2003 for illegal gambling activities; and

v. by reason of the matters set out at subparagraphs a. to u. above, there were real risks that Customer 2's source of wealth/funds were not legitimate.

Monitoring of Customer 2's transactions

786. At no time did Crown Melbourne or Crown Perth appropriately monitor Customer 2's transactions on a risk-basis.

Particulars

Section 36(1)(a), (b) of the Act and rules 15.4 to 15.8 of the Rules.

Crown Melbourne and Crown Perth were unable to monitor the ML/TF risks posed by transactions associated with Customer 2's junkets, including transactions by his junket representatives and key players on his junkets appropriately because they did not make and keep appropriate records of designated services provided: see paragraphs 483ff.

Crown Melbourne and Crown Perth did not apply appropriate risk-based transaction monitoring to designated services provided to Customer 2: see paragraphs 590ff and 629 to 642 (designated services) and 643 to 649 (transactions facilitated through junkets).

Customer 2's transactions involved repeated transactions indicative of ML/TF typologies that were not detected prior to a 2021 lookback. Had appropriate risk-based transaction monitoring been applied, these transactions could have been identified earlier: see paragraphs 686 and 687.

Transactions indicative of ML/TF typologies – quick turnover of funds (without betting)

The following transactions involving Customer 2 were identified as indicative of the ML/TF typology of quick turnover of funds (without betting) by an independent auditor in 2021:

- on 1 July 2018, Customer 2 deposited $30,000 by telegraphic transfer, then withdrew $130,000, $5,000 and $1,900 separately in cash on that same day. This transaction was also identified by the independent auditor as an instance where the total value of

chips redeemed exceeded the total buy-in value within a 48 hour period without sufficient gaming winnings to explain the additional chips redeemed;

- on 26 September 2018, Customer 2 deposited $20,000 and $20,000 by separate cash deposits, then withdrew $26,950 and $20,000 from his DAB on the same day. On 27 September 2018, Customer 2 also withdrew a further $20,000 by telegraphic transfer;
- on 4 March 2019, Customer 2 deposited $200,000 from his DAB account by telegraphic transfer, then withdrew $200,000 in cash on the following day; and
- on 23 April 2019, Customer 2 deposited $300,000 in cash from his DAB account and $100,000 by telegraphic transfer, then withdrew $700,000 by telegraphic transfer on the same day.

Transactions indicative of ML/TF typologies – structuring

The following transactions involving Customer 2 were identified as indicative of the ML/TF typology of structuring by an independent auditor in 2021:

- deposits of $9,800 on 4 January 2019 and $1,500 on 6 January 2019 in cash, within a 72 hour period; and
- deposits on 6 December 2019 of $6,000 and $4,800 in cash, within a 24 hour period.

Transactions indicative of ML/TF typologies – third party transfers

The independent auditor also identified that Customer 2 had made 103 payments to 52 unique third parties, to a total value of $33,209,798.

The independent auditor also noted that on 13 November 2017, Customer 2 had sent $55,000 to a third party who was suspected of involvement in criminal activity.

The following specific transactions involving Customer 2 were identified as involving the risk factor of third party transfers by an independent auditor in 2021:

- Between 3 October 2019 and 19 October 2019, Customer 2 received four payments from third parties through a Southbank account, totalling $300,000.
- Between 14 November 2019 and 18 March 2019, Customer 2 received six payments from third parties through a Crown patron account, totalling $475,000.

Inadequate controls on Crown's private jets

On various occasions in 2018, Crown Melbourne provided Customer 2 with access to a Crown private jet to facilitate travel.

There were inadequate controls on the carrying of large amounts of cash on Crown's private jets*:* see paragraphs 454 and 491(c).

Ongoing customer due diligence

787. On and from 1 March 2016, on multiple occasions, the provision of designated services to Customer 2 at Crown Melbourne and Crown Perth raised red flags reflective of higher ML/TF risks as a result of Customer 2's junket activity.

Particulars

See paragraph 477.

Total gaming activity on junket programs from March 2016 to March 2020

Between March 2016 and March 2020, Customer 2 operated at least 68 junket programs at Crown Melbourne. Crown Melbourne recorded the total turnover of those programs at Crown Melbourne as approximately $10,561,102,323 with losses of approximately $189,720,268. Commissions of $87,571,251 were payable by Crown Melbourne to Customer 2.

Between March 2016 and March 2020, Customer 2 operated at least 4 junket programs at Crown Perth. Crown Perth recorded the total turnover of those programs as approximately $74,123,400 with losses of approximately $5,690,375. Commissions of $587,031 were payable by Crown Perth to Customer 2.

Between March 2016 and March 2020, Crown management regularly reapproved Customer 2's junket credit facility, with limits ranging between $10,000,000 and $20,000,000, as part of a monthly junket review.

Junket activity in 2016

Between March 2016 and June 2016, Customer 2 operated at least 4 junket programs at Crown Melbourne. Crown Melbourne recorded the total turnover on those programs as approximately $600,445,245 with losses of approximately $16,408,255. Commissions of approximately $4,581,983 were payable by Crown Melbourne to Customer 2.

Between January 2016 and December 2016, Crown Melbourne formed suspicions with respect to high losses noted for the key players under Customer 2's junket program, giving the AUSTRAC CEO 10 SMRs that described losses by 21 key players under Customer 2's junket totalling AUD$17,344,578 and HKD$1,854,540: SMRs dated 5 January 2016, 5 February 2016, 6 April 2016, 6 May 2016, 1 June 2016, 1 August 2016, 7 October 2016, 11 November 2016, 1 December 2016, and 16 December 2016.

Between March 2016 and December 2016, Crown management regularly reapproved Customer 2's junket credit facility, up to limits of $20,000,000, as part of a monthly junket review.

Junket activity in 2017

During the 2017 financial year, Customer 2 ran at least 25 junket programs at Crown Melbourne. Crown Melbourne recorded gaming activity in the 2017 financial year on junket programs run by Customer 2 at Crown Melbourne as turnover of approximately $1,541,126,720, with losses of approximately $28,486,858. Commissions of approximately $15,785,496 were payable by Crown Melbourne to Customer 2.

Between March 2017 and December 2017, Crown Melbourne formed suspicions with respect to high losses noted for the key players under Customer 2's junket program, giving the AUSTRAC CEO 8 SMRs that described losses by 27 key players under Customer 2's junket totalling AUD$19,976,680: SMRs dated 1 March 2017, 11 April 2017, 12 May 2017, 9 August 2017, 11 September 2017, 10 October 2017, 10 November 2017 and 12 December 2017.

In 2017, Crown management regularly reapproved Customer 2's junket credit facility, up to limits of $20,000,000, as part of a monthly junket review.

Junket activity in 2018

During the 2018 financial year, Customer 2 ran at least 21 junkets at Crown Melbourne. Crown Melbourne recorded gaming activity in the 2018 financial year on junket programs run by Customer 2 at Crown Melbourne as having turnover of approximately $3,041,678,790 with losses of approximately $51,985,241. Commissions of approximately $24,333,484 were payable by Crown Melbourne to Customer 2.

During the 2018 financial year, Customer 2 ran at least 1 junket program at Crown Perth. Crown Perth recorded gaming activity in the 2017 financial year on junket programs run by Customer 2 at Crown Perth as having turnover of $50,000 and wins of $500. Commissions of $400 were payable by Crown Perth to Customer 2.

Between January 2018 and July 2018, Crown Melbourne formed suspicions with respect to high losses noted for the key players under Customer 2's junket program, giving the AUSTRAC CEO 6 SMRs that described losses by 11 key players under Customer 2's junket totalling AUD$11,280,720: SMRs dated 11 January 2018, 9 February 2018, 22 March 2018, 10 May 2018, 27 June 2018 and 27 July 2018.

In 2018, Crown management regularly reapproved Customer 2's junket credit facility, up to limits of $20,000,000, as part of a monthly junket review.

Junket activity in 2019

During the 2019 financial year, Customer 2 ran at least 8 junkets at Crown Melbourne. Crown Melbourne recorded gaming activity in the 2018 financial year on junket programs run by Customer 2 as having turnover of approximately $3,775,104,760 with losses of

approximately $60,476,779. Commissions of approximately $30,199,478 were payable by Crown Melbourne to Customer 2.

During the 2019 financial year, Customer 2 ran at least 2 junkets at Crown Perth. Crown Perth recorded gaming activity in the 2019 financial year on junket programs run by Customer 2 as having turnover of approximately $13,719,300 with losses of approximately $699,915. Commissions of approximately $103,797 were payable by Crown Perth to Customer 2.

In 2019, Crown management regularly reapproved Customer 2's junket credit facility, up to limits of $20,000,000, as part of a monthly junket review, with the exception of August 2019, when Customer 2's credit facility was suspended on the basis that it would be reactivated once Customer 2 had cleared his $25,000,000 debt owed to Crown. By October 2019, Customer 2's credit facility was reactivated following approvals from Crown management.

Junket activity in 2020

Customer 2 continued to run junkets up until March 2020.

Between January 2020 and March 2020, Crown management regularly reapproved Customer 2's junket credit facility, up to limits of $10,000,000, as part of a monthly junket review.

During the 2020 financial year, Customer 2 ran at least 8 junkets at Crown Melbourne. Crown Melbourne recorded gaming activity in the 2020 financial year on junket programs run by Customer 2 as having turnover of approximately $787,362,040 and losses of approximately $21,059,350. Commissions of approximately $4,389,116 were payable by Crown Melbourne to Customer 2.

During the 2020 financial year, Customer 2 ran at least 1 junket at Crown Perth. Crown Perth recorded gaming activity in the 2020 financial year on junket programs run by Customer 2 as having turnover of approximately $60,354,100 with losses of approximately $4,995,460. Commissions of approximately $482,834 were payable by Crown Perth to Customer 2.

788. On and from 1 March 2016, on multiple occasions, the provision of designated services to Customer 2 at Crown Melbourne and Crown Perth raised red flags reflective of higher ML/TF risks as a result of unusual transactions and patterns of transactions involving Customer 2.

Particulars

See paragraphs 420ff, 450, 451, 456ff, 491.

Unusual transactions and patterns of transactions in 2016

Between April and October 2016, there were eight telegraphic transfers into Customer 2's DAB account at Crown Melbourne from third parties, in circumstances where the third party was not noted as a key player on any of Customer 2's junkets. The deposits totalled AUD$535,000: SMRs dated 27 April 2016, 23 May 2016, 31 May 2016, 22 June 2016 and 19 October 2016.

On around 10 May 2016, Customer 2's representatives liaised with Crown Melbourne to deposit HKD19,000,000 by way of "cash collection" at City of Dreams for the purpose of repaying a credit marker issued by Crown Melbourne (see paragraphs 332ff and 334ff).

On around 31 May 2016, Customer 2's representative, Person 26, arranged for a deposit of HKD10,000,000 at City of Dreams by way of "cash collection". Part of the cash deposited was used to discharge Customer 2's outstanding HKD credit marker (HKD1,322,632) owed to Crown Melbourne, while the remaining HKD8,677,368 was converted to AUD and used to repay the outstanding AUD credit marker owed to Crown Melbourne (see paragraphs 332ff and 334ff).

In May and July 2016, there were two telegraphic transfers withdrawn from Customer 2's DAB account at Crown Melbourne and sent to third parties, in circumstances where either the third party was not a key player on Customer 2's junket or the funds sent did not match the person's rated wins / losses. The withdrawals totalled AUD$714,300: SMRs dated 17 May 2016 and 6 July 2016.

In August 2016, Crown Melbourne gave Customer 2's junket representative, Person 54, a cheque for $200,000 drawing on funds from Customer 2's DAB account, in circumstances where the amount did not match the representative's wins / losses under Customer 2's junket programs: SMR dated 11 August 2016.

On 17 November 2016, Crown Perth sent a telegraphic transfer of $1,000,000, withdrawn from another junket operator's DAB account (Customer 11) which was deposited into Customer 2's DAB account at Crown Melbourne: 22 November 2016.

Unusual transactions and patterns of transactions in 2017

Between January 2017 and December 2017, there were at least 14 telegraphic transfers into Customer 2's DAB account at Crown Melbourne from third parties in circumstances where either the third party was not a key player on Customer 2's junket or the funds sent did not match the person's rated wins / losses. The deposits totalled $8,653,900: SMRs dated 24 January 2017, 27 April 2017, 15 June 2017, 19 June 2017, 21 August 2017, 22 August 2017, 4 September 2017, and 6 December 2017.

In March 2017, Crown Melbourne sent $300,000 via telegraphic transfer from Customer 2's DAB account to a third party, in circumstances where the third party was not noted as a key player on any of Customer 2's junkets: SMR dated 23 March 2017.

Between September and October 2017, there were two instances of suspicious cash transactions by representatives of Customer 2's junket. On 10 September 2017, Customer 2's junket representative, Person 50, presented a paper bag of cash in various denominations, which amounted to $199,950. Customer 2's junket representative then provided a further $50 note, taking the cash to $200,000 and

informed the Cage that the cash was from the home of a key player: SMR dated 11 September 2017. On 31 October 2017, another Customer 2 junket representative presented cash totalling $100,000, in $10,000 bundles of $50 notes wrapped in rubber bands, claiming that the cash was provided by a key player, who was not identified, as repayment for funds he had lost: SMR dated 1 November 2017.

On 11 September 2017, $2,732,581 was transferred from Customer 2's DAB account to another Crown patron, Customer 21, who was not a key player under any of Customer 2's junkets but had an extensive history of significant annual losses at Crown Melbourne: SMR dated 1 September 2017.

On 29 November 2017, there were two telegraphic transfers of $90,000 and $144,000 deposited into the DAB accounts of two different Crown patrons. These amounts were immediately transferred from those accounts to Customer 2's DAB account, in circumstances where neither patron was noted as a key player on any of Customer 2's junkets: SMR dated 30 November 2017.

On 29 November 2017 and 1 December 2017, Crown Melbourne identified that two of Customer 2's key players engaged in transactions for the purchase of gaming chips at similar times, obtaining chips totalling $110,000, despite both players having minimal rated gaming activity: SMR dated 4 December 2017.

In November and December 2017, Crown Melbourne sent six telegraphic transfers from Customer 2's DAB account at Crown Melbourne to third parties, in circumstances where either the third party was a company, or was not noted as a key player on Customer 2's junket. The withdrawals totalled $1,755,000: SMRs dated 6 November 2017, 8 November 2017, 14 November 2017 and 18 December 2017.

Unusual transactions and patterns of transactions in 2018

Between January 2018 and December 2018, there were at least 186 telegraphic transfers into Customer 2's DAB account at Crown Melbourne from third parties in circumstances where the third party was not a key player on Customer 2's junket. The deposits totalled $25,428,721. The majority of telegraphic transfers were deposited by the same ten individuals, including Person 9, Person 15, and Person 17.

In addition to the numerous telegraphic transfers received and deposited into Customer 2's DAB account, the following unusual or suspicious transactions occurred in 2018.

In January and February 2018, there were seven suspicious cash transactions involving Customer 2's junket representatives, including:

- on 3 January 2018, Customer 2's junket representative, Person 50, requested to deposit $420,000 in cash wrapped in plastic into Customer 2's DAB account, and refused to disclose whether the

money related to a particular patron or where the money came from: SMR dated 3 January 2018;

- on 9 January 2018, Customer 2's junket representative, Person 50, presented $230,000 and $70,000 in cash in bundles of $10,000 in $50 notes that did not appear to have been issued from a bank or at the Cage, and informed Crown that the cash was from a key player on Customer 2's junket. The cash was deposited into Customer 2's DAB account: SMR dated 10 January 2018;
- on 26 January 2018, Customer 2's junket representative, Person 50, presented $100,000 in bundles of $10,000 in $50 notes, informed Crown that the cash was from a key player on Customer 2's junket (the same key player as referred to in the paragraph immediately above), but he did not know where the player had got the funds from. The cash was deposited into Customer 2's DAB account: SMR dated 29 January 2018;
- on 1 February 2018, Customer 2's junket representative, Person 50, presented $185,000 in bundles of $10,000 in $50 notes, and exchanged the cash for gaming chips: SMR dated 2 February 2018;
- on 9 February 2018, Customer 2's junket representative, Person 50, presented $140,000 in cash in $100 notes, wrapped in rubber bands, and informed Crown that the cash was from a key player. The cash was exchanged for gaming chips which were then provided to friends of the key player: SMR dated 12 February 2018;
- on 13 January 2018, Customer 2's junket representative, Person 50, withdrew $120,000 (which had been deposited into Customer 2's DAB account via telegraphic transfer that day) in gaming chips, then later exchanged the chips for cash without any gaming. Shortly afterwards, a third party, Customer 22, presented $120,000 in cash for deposit into his own DAB account: SMR dated 15 January 2018; and
- on 16 January 2018, Customer 2's junket representative, Person 50, attended the Cage with a receipt for a cash deposit for $300,000, which had been sent to Crown that day, and requested to access the funds. The Cage advised the representative that the funds wouldn't be able to be accessed until received the following day. The SMR recorded suspicions that the funds related to Customer 22: SMR dated 17 January 2018.

In March 2018 and April 2018, Crown Melbourne sent two telegraphic transfers from Customer 2's DAB account at Crown Melbourne to two different third party companies. The withdrawals totalled: $569,300: SMRs dated 1 March 2018 and 27 April 2018.

On 17 April 2018, Customer 2's junket representative, Person 50, presented $150,000 in cash (made up of $40,000 in $100 notes and

$110,000 in $50 notes) to exchange for cash chips, instead of commission-based chips regularly used by junkets: SMR dated 18 April 2018.

On 9 May 2018, Crown Melbourne sent a telegraphic transfer of $1,000,000 from Customer 2's DAB account to a third party, who was not noted at the time as a key player on any of Customer 2's junkets: SMR dated 10 May 2018.

On 18 July 2018, Crown Melbourne received a deposit of $129,000 from a third party, with a reference "purchase of car", that was to be deposited into Customer 2's DAB account. Crown Melbourne returned the funds to the depositor on the basis of the reference to the purchase of the car: SMR dated 19 July 2018.

Over July and August 2018, Customer 2's junket representative, Person 50, engaged in three suspicious cash transactions:

- on 26 July 2018, the representative presented $175,000 in cash made up of $50 and $100 notes, and a $25,000 gaming chip, and exchanged this for gaming chips. The representative then produced a further $275,000 in cash (understood to belong to a key player on Customer 2's junket) for deposit into Customer 2's DAB account, of which $105,000 was ultimately deposited into the account: SMR dated 2 August 2018;
- on 2 August 2018, the representative deposited $300,000 in cash into Customer 2's DAB account, which Crown suspected was the part of a cash withdrawal of $480,000, which had been withdrawn from Customer 4's DAB account by a Customer 4 junket representative earlier that day: SMR dated 3 August 2018; and
- on 24 August 2018, the representative presented two dusty Crown bags containing $100,000 in cash made up of $45,000 in $100 notes and $55,000 in $50 notes, for deposit into Customer 2's DAB account: SMR dated 27 August 2018.

On 4 December 2018, Customer 2's junket representative, Person 50, presented $100,000 in cash, informing Crown that it came from a key player, who was showing significant losses under Customer 2's junket program: SMR dated 5 December 2012.

Unusual transactions and patterns of transactions in 2019

Between January 2019 and December 2019, there were at least 231 telegraphic transfers into Customer 2's DAB account at Crown Melbourne from third parties in circumstances where the third party was not a key player on Customer 2's junket. The deposits totalled $36,301,780. The majority of telegraphic transfers were deposited by the same individuals, including: Person 9, Person 15, Person 17 and six others.

On 10 April 2019, a third party deposited $400,000 of gaming chips into his Crown DAB account, which was immediately transferred to Customer 2's DAB account. A few weeks later, the same third party

exchanged $65,000 in gaming chips for cash, despite his rated gaming not supporting the transaction: SMR dated 27 June 2019.

By late July and early August 2019, Customer 2 was in debt to both Crown Melbourne and Crown Perth, arising from outstanding credit markers drawn for $20,000,000 at Crown Melbourne ($15,000,000 owing since 17 June 2019 and $5,000,000 owing since 29 July 2019), and $5,000,000 at Crown Perth (owing from 2 August 2019). As a result, Crown temporarily suspended Customer 2's credit facility until he had cleared the some of the debt.

On 30 July 2019, $2,000,000 was transferred from Customer 1's DAB account to Customer 2's DAB account, which gave rise to a suspicion based on the transfer of funds between two junket operators: SMR dated 31 July 2019.

Between 29 July 2019 and 8 August 2019, Crown received ten telegraphic transfers of funds, to be deposited into the Customer 2 DAB account, which were initially deposited in cash at various branches in the western Sydney region, in the following amounts: $50,000, $30,000, $30,000, $30,000, $30,000, $30,000, $35,000, $35,000 $35,000 and $35,000. Customer 2's junket representative, Person 26, was not aware of the deposits and did know who deposited the funds: SMR dated 9 August 2019.

Between 12 August and 19 August 2019, the Group General Manager (International Business Operations) was regularly informed of payments made into Crown for the benefit of Customer 2, which were being tracked for the purpose of reconciling payments against the outstanding debt owed to Crown Melbourne and Crown Perth. Between 5 August 2019 and 19 August 2019, Crown had recorded 44 separate deposits via cash deposits or telegraphic transfers were received from third parties, totalling $7,216,000.

On 16 August 2019, Crown Perth received a telegraphic transfer from Crown Melbourne, withdrawn from Customer 2's DAB account, of $4,517,166.

By September 2019, Crown staff noted that the numerous telegraphic transfers received from third parties for the benefit of Customer 2 were being deposited into Customer 2's DAB account, despite a comment in SYCO that the transfers should be used to pay down outstanding credit markers because staff were reluctant to 'upset' Customer 2's junket representative, Person 26.

In October 2019, Customer 2's junket representative sought approval from Crown Melbourne's senior management for an 'early release of funds' comprising two telegraphic transfers totalling $510,000 and a bank cheque of $3,000,000 as part of an arrangement to repay the debt owed to Crown Melbourne, while also drawing down on further credit for a new junket program.

By 11 November 2019, the Group General Manager (International Business Operations) and Senior Vice President (International

Business), were informed about third party payments received by Crown Melbourne for the benefit of Customer 2 between 5 August 2019 and 7 November 2019, which were being tracked for the purpose of reconciling payments against the outstanding debt owed to Crown Melbourne and Crown Perth and which totalled $15,150,500.

On 30 December 2019, Crown Melbourne's AML Manager requested information from another Crown staff member about four of the third parties who had been depositing funds with Crown for the benefit of Customer 2 via telegraphic transfer in December 2019, and queried their relationship to Customer 2 or any of the key players. In response, the Senior Vice President (International Business Operations) noted that he had discussed this with Customer 2's junket representative, who had indicated that the third parties were known to him and were assisting in transferring funds to settle outstanding credit markers owed to Crown Melbourne, and stated that it is challenging to obtain better information 'without pushing too hard' because 'it has not been a requirement in the past to have these details documented'. Crown Melbourne did not record any further steps taken to inquire about the four third parties.

Unusual transactions and patterns of transactions in 2020

Between January 2020 and March 2020, there were at least 27 telegraphic transfers into Customer 2's DAB account at Crown Melbourne from third parties in circumstances where the third party was not a key player on Customer 2's junket. The deposits totalled $5,187,600. The majority of telegraphic transfers were deposited by the same individuals, including Person 17 and four others.

789. On and from 1 March 2016, the provision of designated services by Crown Melbourne and Crown Perth to Customer 2 posed higher ML/TF risks in circumstances where Crown Melbourne and Crown Perth were aware of publicly available information in relation to Customer 2.

Particulars

2016 media allegations

By 12 December 2016, Crown obtained a risk intelligence report, which reported the following matters:

- in 2003, foreign media reported that Customer 2 and his associate Person 54 (who was Customer 2's junket representative at Crown Melbourne) had been sentenced to 2 years and 8 months imprisonment on 1 August 2003, following convictions for illegal gambling activity. The proceeds of illegal gambling activity were confiscated. The associate referred to in the articles was Customer 2's junket representative at Crown Melbourne (Person 26); and
- in 2016, a law enforcement agency had filed an application for examination orders in relation to a car purchased using $747,000

sent from Customer 2's DAB account on 16 December 2012. The basis of the application was the agency's suspicion that the car was purchased using the proceeds of crime relating to money-laundering or tax avoidance.

By 20 December 2016, Crown obtained a media article dated 19 December 2016, which reported that on 3 December 2016, a foreign political leader had ordered the arrest of Customer 2's business associate, Person 14, alleging that he had attempted to bribe public officials to release foreign nationals arrested in a foreign country for illegal gambling. The media report was provided to the Chief Executive Officer (Australian Resorts), Senior Vice President (International Business), Group General Manager (International Business Operations) and the Executive General Manager, Legal & Regulatory Services, Crown Melbourne and a Crown Resorts director.

By 22 December 2016, Crown obtained a copy of the foreign media report dated 1 August 2003, which reported on Customer 2's alleged conviction and imprisonment for illegal gambling activities.

August 2019 media allegations

On 2 August 2019, an article published by an Australian media outlet alleged that Customer 2 had been named in foreign court records dated 2003 as having led a violent organised crime group and illegal gambling syndicate that engaged in extortion and violence, as well as being named in a 2016 proceeds of crime case in an Australian court that alleged that Customer 2's junket operations were involved money laundering and tax avoidance. The article was obtained by Crown and incorporated into Customer 2's junket profile as at 20 September 2019.

February 2021 – Bergin Report

The Bergin Report found that that allegation that Customer 2 was convicted and imprisoned in 2003 was "probably true" and that it is "probable" that the Customer 2 junket had the organised crime links as alleged.

April 2021 – VCGLR Show Cause Decision

On 2 October 2020, the VCLGR issued a show cause notice issued with respect to Customer 2, alleging that Crown Melbourne had failed to verify open-source media reports that Customer 2 had been convicted of being part of a large illegal gambling syndicate and that it failed to have proper regard to Customer 2's involvement in a proceeds of crime case before an Australian court. The show cause notice also referred to other individuals, including Customer 1, Customer 26 and Customer 32. On 27 April 2021, the VCGLR concluded that Crown Melbourne had breached section 121(4) of the *Casino Control Act* and imposed the maximum fine of $1,000,000.

790. On and from 1 March 2016, on multiple occasions, enquiries by law enforcement agencies relating to Customer 2 raised red flags reflective of higher ML/TF risks for the provision of designated services to Customer 2 at Crown Melbourne.

Particulars

On 16 November 2016, an enquiry by law enforcement was made in respect of Customer 2.

On 15 December 2017, an enquiry by law enforcement was made in respect of Customer 2.

791. At no time did Crown Melbourne or Crown Perth undertake appropriate risk-based customer due diligence with respect to Customer 2 with a view to identifying, mitigating and managing the ML/TF risks posed by the provision of designated services on and from 1 March 2016.

a. At no time did Crown Melbourne or Crown Perth take appropriate steps to understand Customer 2's source of wealth/funds was legitimate.

b. At no time did Crown Melbourne or Crown Perth take appropriate steps to identify or analyse the ML/TF risks of Customer 2's transactions or to consider whether they had a lawful purpose.

c. With the exception of the telegraphic transfer of $129,000 on 18 July 2018 which contained a reference to the purchase of a car and was returned to the depositor, Crown Melbourne gave no consideration at any time to whether large and high risk transactions should be processed.

d. At no time did Crown Perth give appropriate consideration to whether large and high risk transactions should be processed.

e. On each occasion prior to January 2021 that senior management considered whether to continue the business relationship with Customer 2, senior management failed to give adequate consideration to whether the ML/TF risks posed by Customer 2 were within Crown Melbourne and Crown Perth's risk appetite.

Particulars

Section 36(1)(a) of the Act.

The due diligence steps taken with respect to Customer 2 included:

Database searches

On 12 August 2016, 11 December 2016, 1 April 2018, 12 June 2018, 27 September 2018, 19 March 2019, 28 July 2019, 2 August 2019, 13 August 2019, 8 January 2020, Crown performed risk intelligence searches on Customer 2.

On 31 March 2016, 12 December 2016, 6 February 2017, 10 February 2017, 11 May 2018, 21 May 2018, 3 January 2019, 19 March 2019, 2 April 2019, 23 May 2019, 27 July 2019, Crown performed various property and corporate searches, including company and bankruptcy searches, which disclosed details regarding companies and properties associated with Customer 2 and his associates.

Crown conducted open source searches on the following occasions, obtaining the following:

- on 20 December 2016, a media article dated 19 December 2016 which reported on the ordered arrest of Customer 2's business associate, Person 14, for attempted bribery;
- on 22 December 2016, a foreign media report dated 1 August 2003, which reported on Customer 2's conviction and imprisonment for illegal gambling activities;
- on 1 August 2019, media report searches for Customer 2's name and other key words including 'laundering';
- on 9 September 2019, a media article dated 2 August 2019, which referred to Customer 2's alleged 2003 conviction and involvement in the 2016 proceeds of crime case before an Australian court;
- on 23 September 2019, a media article dated 21 October 2016 referring to the 2016 proceeds of crime case before an Australian court but which did not directly name Customer 2; and
- on 19 March 2020, translated copies of foreign media articles reporting on Customer 2's alleged conviction and imprisonment for illegal gambling activities in a foreign country.

Wealth information

On 12 December 2016, Crown Melbourne and Crown Perth obtained a wealth report in respect of Customer 2 to obtain information relevant for inclusion in the junket profiles to assess Customer 2's financial position. The report referred to Customer 2's alleged 2003 conviction and imprisonment in a foreign jurisdiction, the Australian proceeds of crime court proceedings in 2016, and listed associates with alleged links to criminal activity, including Customer 2's junket representative at Crown Melbourne (Person 26).

Additional wealth reports were obtained on 8 March 2019, 2 April 2019, and 24 April 2020 for the purposes of assessing credit risk.

On 23 August 2019, Crown Melbourne and Crown Perth obtained a wealth report which set out information about Customer 2's estimated net worth through shareholdings and companies, which also: noted that Customer 2 held shares in a company registered at an address listed in open source databases as related to an organised cybercrime gang; referred to adverse media on Customer 2; and listed Customer 2's associates who posed risks due to adverse media or law enforcement issues.

Junket reviews

On 13 December 2016, the Credit control team drafted a junket profile in respect of Customer 2 and his junket operations that summarised the findings of a wealth report obtained on 12 December

2016, including reported allegations regarding Customer 2's 2003 criminal history and links to the 2016 proceeds of crime matter.

Customer 2's junket profile was updated with details of the database searches and wealth information outlined above on 4 January 2017, 9 June 2017, 14 August 2017, 13 June 2018, 31 July 2019, 26 August 2019, 9 September 2019, 20 September 2019, 13 December 2019, 14 July 2020. Each profile recommended that Crown continue to conduct business with Customer 2, but did not provide a basis for this decision.

Senior management engagement

Senior management directly considered Crown Melbourne and Crown Perth's relationship with Customer 2 on the following occasions.

On 20 December 2016, a VIP Operations Committee meeting attended by the Senior Vice President (International Business), a Crown Resorts director, Group General Manager (International Business Operations), Chief Executive Officer (Australian Resorts) and the Executive General Manager, Legal and Regulatory, considered a copy of Customer 2's junket profile and a media article recording the order for arrest of Customer 2's business associate, Person 14, and requested further information about the adverse media described in the profile.

On 4 January 2017, a VIP Operations Committee meeting attended by the Senior Vice President (International Business), a Crown Resorts director, Group General Manager (International Business Operations), Chief Executive Officer (Australian Resorts) and Executive General Manager, Legal and Regulatory, Group General Counsel, Crown Resorts and Chief Executive Officer (Crown Resorts), considered an updated copy of Customer 2's junket profile and resolved to have Crown staff speak with Customer 2 about the reported 2003 conviction and his junket representative to give Crown comfort to continue conducting business with Customer 2's junket. There was no record of Crown asking Customer 2 directly about the 2003 conviction.

On 23 July 2019, Crown Resorts received an Australian media enquiry which contained allegations that Customer 2 was connected to organised crime in Australia and overseas. On 2 August 2019, an article was published by an Australian media outlet which referred to Customer 2 as a junket operator at Crown and referred to his alleged 2003 conviction and links to the 2016 proceeds of crime case before an Australian court.

On 20 August 2019, the Chief Legal Officer prepared an updated memorandum to the Board of Crown Resorts, which outlined Customer 2's junket activity at Crown Melbourne and Crown Perth. The memorandum noted that recent media and risk intelligence searches had returned no results, and that the wealth reports (which

contained reports on Customer 2's alleged conviction in 2003) contained "nothing adverse". At the time, Customer 2 owed a debt of around $25,000,000 to Crown Melbourne. Crown Melbourne was receiving payments from a number of third parties (in cash and via telegraphic transfer) for the benefit of Customer 2 and to discharge the debt.

On 10 June 2020, the Chief Legal Officer wrote to the Chief Executive Officer, Australian Resorts and Chief Executive Officer, Crown Resorts providing an update to earlier emails sent in March 2020 regarding Customer 2 and another junket operator, Customer 1. The email referred to analysis of activity on the Customer 2 junket and noted that a memorandum on next steps would be prepared.

On 25 June 2020, the Chief Legal Officer advised the Chief Executive Officer, Australian Resorts and Chief Executive Officer, Crown Resorts by memorandum that Crown should reassess its relationship with Customer 2 and seek advice from a law firm on the risks of continuing to do business with Customer 2. The Chief Legal Officer advised that any due diligence exercises should also focus on Customer 2's junket representative, Person 26.

On 12 September 2020, Crown obtained a report by an independent expert in relation to Customer 2, which noted the following key issues:

- Customer 2's companies are used to support junket operations by bringing 'high rollers' overseas and helping to move capital;
- Customer 2 was affiliated with a sub-junket group (along with his father-in-law), which sat under a larger foreign junket group, which sources alleged to be associated with a bank that had been investigated in 2005 for suspected banking with certain sanctioned foreign countries;
- Customer 2's 2003 conviction in a foreign jurisdiction arose out of the operation of over 300 illegal gambling games in remote fish farms and warehouses; and
- in addition to representing Customer 2's junket, junket representative, Person 26, also acted as a liaison for the Suncity junket and the Chinatown junket.

At no time between 2016 and 2020 did senior management give adequate consideration to the ML/TF risks posed by Customer 2 and whether an ongoing business relationship was within Crown Melbourne or Crown Perth's its risk appetite.

January 2021 POI Committee and WOL

On 20 January 2021, the Crown Resorts POI Committee considered Customer 2, who had come to the Committee's attention through the ILGA inquiry. The Committee agreed to apply a WOL against Customer 2.

On 22 January 2021, the WOL took effect at Crown Melbourne.

On 29 January 2021, the NRL took effect at Crown Perth.

Prior to January 2021, none of these steps were proportionate to the ML/TF risks reasonably posed by Customer 2 on and from 1 March 2016.

Enhanced customer due diligence

792. Having formed a suspicion for the purposes of s41 of the Act, Crown Melbourne gave the AUSTRAC CEO SMRs with respect to Customer 2 on the occasions listed in Schedule 3.2.

Particulars

The SMRs reported on:

- annual losses by key players on Customer 2's junkets;
- Customer 2's telegraphic transfers with third parties; and
- large cash deposits and withdrawals from Customer 2's DAB account.

793. On each occasion that Crown Melbourne formed a suspicion with respect to Customer 2 for the purposes of s41 of the Act, it was required to apply its ECDD program to Customer 2.

Particulars

Rule 15.9(3) of the Rules.

794. Crown Melbourne did not carry out appropriate risk-based ECDD measures with respect to Customer 2 on each occasion that Crown Melbourne formed a suspicion with respect to Customer 2 for the purposes of s41 of the Act.

a. With the exception of the SMR given to the AUSTRAC CEO on 1 January 2020, there are no records of ECDD being conducted after the SMRs were given between 27 April 2016 and 20 March 2020: see paragraphs 664 and 685.

b. Appropriate risk-based steps were not taken to obtain or analyse information about Customer 2's source of wealth/funds: see paragraph 667.

c. Appropriate risk-based steps were not taken to analyse and monitor Customer 2's transactions – both past and future – including to understand their economic purpose: see paragraphs 590 and 666.

d. On each occasion prior to January 2021 that senior management considered whether to continue the business relationship with Customer 2, senior management failed to give adequate consideration to whether the ML/TF risks posed by Customer 2 were within Crown Melbourne's risk appetite: see paragraph 668ff.

Particulars

Rule 15.9(3), Rule 15.10(1)(c), (d), (2), (5) and (6) of the Rules.

Prior to giving the AUSTRAC CEO an SMR on 1 January 2020, on 31 December 2019, the AML Manager performed risk intelligence searches for Customer 2 and the transferor, with no results returned.

See the particulars to paragraph 791.

795. Having formed a suspicion for the purposes of s41 of the Act, Crown Perth gave the AUSTRAC CEO SMRs with respect to Customer 2 on 22 November 2016.

Particulars

The SMR reported a large telegraphic transfer from a junket operator Customer 11 to Customer 2's Crown Melbourne DAB account.

796. On each occasion that Crown Perth formed a suspicion with respect to Customer 2 for the purposes of s41 of the Act, it was required to apply its ECDD program to Customer 2.

Particulars

Rule 15.9(3) of the Rules.

797. Crown Perth did not carry out appropriate risk-based ECDD measures with respect to Customer 2 on each occasion that Crown Perth formed a suspicion with respect to Customer 2 for the purposes of s41 of the Act.

a. There are no records of ECDD being conducted after giving the AUSTRAC CEO the SMR on 22 November 2016: see paragraphs 664 and 685.

b. Appropriate risk-based steps were not taken to obtain or analyse information about Customer 2's source of wealth/funds: see paragraph 667.

c. Appropriate risk-based steps were not taken to analyse and monitor Customer 2's transactions – both past and future – including to understand their economic purpose: see paragraphs 590 and 666.

d. On each occasion prior to January 2021 that senior management considered whether to continue the business relationship with Customer 2, senior management failed to give adequate consideration to whether the ML/TF risks posed by Customer 2 were within Crown Perth's risk appetite: see paragraph 668ff.

Particulars

Rule 15.9(3), 15.10(1)(c), (d), (2), (5) and (6) of the Rules.

See the particulars to paragraph 791.

798. By reason of the matters pleaded from paragraphs 772 to 797, on and from 1 March 2016, Crown Melbourne and Crown Perth:

a. did not monitor Customer 2 in relation to the provision of designated services, with a view to identifying, mitigating and managing the ML/TF risks reasonably faced; and

b. did not do so in accordance with r15.5 and 15.9 of the Rules.

799. By reason of the matters pleaded at paragraph 798, Crown Melbourne contravened s36(1) of the Act on and from 1 March 2016 to 22 January 2021 with respect to Customer 2.

Particulars

Section 36(1) of the Act is a civil penalty provision: s36(2) of the Act.

800. By reason of the matters pleaded at paragraph 798, Crown Perth contravened s36(1) of the Act on and from 1 March 2016 to 29 January 2021 with respect to Customer 2.

Particulars

Section 36(1) of the Act is a civil penalty provision: s36(2) of the Act.

Customer 3

801. Customer 3 has been a customer of Crown Melbourne from 9 December 2014 to 12 November 2021.

802. From at least 9 December 2014 to 12 November 2021, Crown Melbourne provided Customer 3 with designated services within the meaning of table 1 and table 3, s6 of the Act.

803. From at least 9 December 2014 to 22 January 2021, Customer 3 received designated services as a junket operator of the Meg-Star junket at Crown Melbourne and as a key player in his own junket program.

Particulars to paragraphs 802 and 803

Customer 3 was the junket operator and ultimate beneficial owner of the Meg-Star junket.

On and from at least 4 September 2009, Crown signed NONEGPRAs with Customer 3. On 1 August 2019, Crown Melbourne and Crown Perth entered into a further NONEGPRA with Customer 3 to operate junkets at Crown Melbourne and Crown Perth.

On various occasions, Customer 3 was allocated 13 PIDs at Crown Melbourne.

On 9 December 2014, Crown Melbourne opened a credit facility (AUD/HKD) for Customer 3. Customer 3 had a credit limit of $500,000 established at the time. This credit facility was closed on 24 November 2020.

On 10 December 2014, Crown Melbourne opened a DAB account and safekeeping account (AUD/HKD) for Customer 3 under two PIDs. Crown Melbourne opened a further six DAB account and safekeeping accounts for Customer 3 on 23 February 2015, 17 April 2017, 14 February 2018, 20 February 2018, 7 June 2018 and 17 December 2019. These accounts were each closed on 12 November 2021.

On 18 February 2020, Crown Melbourne opened an eighth DAB account and safekeeping account (AUD) under a further PID. The accounts were closed on 24 November 2020.

On 20 January 2021, the Crown Resorts POI Committee considered Customer 3, who had come to the Committee's attention through the ILGA inquiry, and agreed to apply a WOL to Customer 3.

On 22 January 2021, the WOL took effect at Crown Melbourne. However, his DAB account and safekeeping accounts were not closed under 12 November 2021.

Between 13 April 2016 and 23 March 2020, Customer 3 operated 221 Meg-Star junket programs at Crown Melbourne: 50 under an initial PID, 38 under a second PID, two under a third PID, one under a fourth PID, 41 under a fifth PID, 41 under a sixth PID, 21 under a seventh PID and 27 under an eight PID. In that period, Customer 3 had approximately 149 junket representatives, including Customer 3 and Customer 26.

By December 2020, the Meg-Star junket had a cumulative turnover at Crown Melbourne of $10,000,000,000 with a cumulative loss of $60,000,000.

Between 2014 and 2017, Crown Melbourne recorded Customer 3's individual rated gaming activity as being a cumulative loss of $19,849.

804. Customer 3 has been a customer of Crown Perth from 8 February 2015 to 29 January 2021.

805. Between 8 February 2015 and 29 January 2021, Crown Perth provided Customer 3 with designated services within the meaning of table 1 and table 3, s6 of the Act.

806. Between 8 February 2015 and 29 January 2021, Customer 3 received designated services as a junket operator of the Meg-Star junket and junket representative at Crown Perth.

Particulars to paragraphs 805 and 806

Customer 3 was the junket operator of the Meg-Star junket.

On and from at least 4 September 2009, Crown signed NONEGPRAs with Customer 3. On 1 August 2019, Crown Melbourne and Crown Perth entered into a further NONEGPRA with Customer 3 to operate junkets at Crown Melbourne and Crown Perth.

On various occasions, Customer 3 was allocated 15 PIDs at Crown Perth.

On 8 February 2015, Crown Perth opened a FAF (AUD/HKD) for Customer 3 under two PIDs. Customer 3 had a credit limit of $10,000,000 established at this time. This FAF was closed on 24 November 2020.

On 9 February 2015, Crown Perth opened a DAB account and safekeeping account (AUD/HKD) for Customer 3 under two PIDs. Crown Perth opened a further three DAB account and safekeeping accounts for Customer 3 on 17 May 2018, 7 June 2018 and 2 March 2019. These account remains open.

On 7 June 2018, Crown Perth opened a second FAF account (AUD) for Customer 3 under a further PID. This account remains open.

On 29 January 2021, Crown Perth issued an NRL with respect to Customer 3.

Between 10 July 2016 and 23 February 2020, Customer 3 operated 61 junket programs at Crown Perth: 36 under one PID, 16 under a second PID, eight under a third PID and one under a fourth PID. In that period, Customer 3 had 25 junket representatives.

By December 2020, the Meg-Star junket had a cumulative turnover at Crown Perth of $442,000,000 with a cumulative loss of $11,000,000.

As at 19 February 2022, Customer 3 had a Crown Perth DAB balance of $55,976.

The ML/TF risks posed by Customer 3

807. By 1 March 2016, higher ML/TF risks were indicated by the nature and purpose of Customer 3's business relationship with Crown Melbourne and Crown Perth, the nature of the transactions he had been conducting, together with the suspicions Crown Melbourne itself had formed with respect to Customer 3.

Particulars

Section 36(1)(a), (b) of the Act and Chapter 15 of the Rules.

Customer 3 was a junket operator. He received designated services through the channel of junket programs. This channel lacked transparency: see paragraph 477.

SMRs

By 1 March 2016, Crown Melbourne had given the AUSTRAC CEO five SMRs in relation to Customer 3 – on 10 March 2015, 13 July 2015, 17 August 2015, 18 November 2015 and 26 February 2016. Each SMR reported the same repeated patterns of significant losses of junket players in the Meg-Star junket. On each occasion, the total loss in the junket was equal to the total loss of the individual player the subject of the SMR, indicating that there was a single key player in each junket program.

Junket activity

In FY2015, Crown Melbourne recorded that the Meg-Star junket had a turnover of $15,212,860 and a win of $416,838.

On various occasions between 11 March 2015 and 12 February 2016, Crown Melbourne prepared a credit profile and obtained a central credit check in respect of Customer 3 for the purpose of extending the Meg-Star junket a line of credit, which varied between $500,000 and $1,000,000 throughout that period.

In FY2015, Crown Melbourne recorded that the Meg-Star junket had a turnover of $90,662,700 with a win of $10,051,040. The Meg-Star junket did not have any recorded turnover in FY2016.

On various occasions between 1 May 2015 and 6 January 2016, Crown Perth prepared a credit profile in respect of Customer 3 for the purpose of extending the Meg-Star junket a line of credit, which was $10,000,000 throughout that period.

Large and suspicious transactions

On 12 March 2015, Customer 3 sent a telegraphic transfer to his Crown Perth DAB account of $9,081,040 for the purpose of settling a debt at Crown Perth.

Other red flags

In 2014 and 2015, Crown Melbourne recorded Customer 3's individual rated gaming activity as net loss of $89,240.

By 2014, Crown Melbourne was aware that the Meg-Star International Company Limited (**Meg-Star International Ltd**) had received investment of about $2,500,000 from a known member of a crime syndicate.

Customer 3 engaged in transactions that were identified by an independent auditor in 2021 as indicative of ML/TF typologies involving quick turnover of funds on at least one occasion. On 1 May 2015, Customer 3 deposited $42,683 by telegraphic transfer into his Crown Melbourne DAB account followed by a withdrawal of the same sum on the same day.

Due diligence conducted by 1 March 2016

By 1 March 2016, the due diligence steps taken with respect to Customer 3 included Crown obtaining a due diligence report from Melco Crown Entertainment, which identified Customer 3 and his brothers to be the central figures of a foreign junket operator, Meg-Star International Ltd, together with his business interests and property holdings.

In October 2014, Crown Melbourne obtained wealth reports in respect of Customer 3, which identified Customer 3's business interests, including his relationship with Meg-Star, that his net worth was at least $11,000,000 and that he had formerly been an executive with the international junket operator Suncity and was associated with Customer 1.

Crown conducted open source searches in respect of the international junket operator Meg-Star, which identified Customer 3's ownership interests in the junket operator, that Meg-Star had previously acquired a Suncity entity and Customer 3's business holdings.

Crown also conducted risk intelligence searches.

808. At all times from 1 March 2016, Customer 3 was a foreign PEP.

Particulars

Customer 3 was a foreign PEP by association with his brother, who was a member of a foreign political body.

809. At all times on and from 1 March 2016, Customer 3 should have been recognised by Crown Melbourne and Crown Perth as a high risk customer by reason of the matters pleaded at paras 807, 808, 812, 813, 814, 815, 816, 817, 819, 820 and 823.

Particulars

Section 36(1)(a), (b) of the Act and Chapter 15 of the Rules.

810. It was not until 5 April 2017 that Customer 3 was rated high risk by Crown Melbourne.

Particulars

On various occasions between 7 January 2015 and 4 April 2017, Crown Melbourne assessed Customer 3 as significant risk.

This was despite:

- the Meg-Star junket's very high turnover as at 1 March 2016;
- that the Meg-Star junket had facilitated multiple junket programs with only a single key player; and
- that open source media reports connected Meg-Star International Ltd with organised crime.

It was not until 5 April 2017 that Crown Melbourne rated Customer 3's risk as high. On various occasions between 5 April 2017 and 16 February 2021, Crown Melbourne rated Customer 3's risk as high.

See paragraph 481.

811. It was not until 20 January 2021 that Customer 3 was rated high risk by Crown Perth.

Particulars

Crown Perth did not designate Customer 3 with a risk rating until 6 July 2018. On various occasions between 6 July 2018 and 19 January 2021, Crown Perth assessed Customer 3 as low risk.

This was despite:

- the Meg-Star junket's very high turnover as at 1 March 2016;
- the significant credit extended to the Meg-Star junket by Crown Perth; and
- that open source media reports connected Meg-Star International Ltd with organised crime.

It was not until 20 January 2021 that Crown Perth rated Customer 3's risk as high. On various occasions between 20 January 2021 and 31 July 2021, Crown Perth assessed Customer 3 as high risk.

See paragraph 481.

812. On and from 1 March 2016, designated services provided to Customer 3 posed higher ML/TF risks including because the provision of designated services to Customer 3 involved a combination of the following factors:

a. Customer 3 was a junket operator who facilitated the provision of high value financial and gaming services (tables 1 and 3, s6) to many key players (including foreign PEPs) through the Meg-Star junket: see paragraph 473ff;

b. Customer 3 was the junket operator and ultimate beneficial owner of the Meg-Star junket;

c. Customer 3 was the founder and chairman of Meg-Star International Ltd which operated eight VIP clubs associated with gambling activities in foreign countries;

d. Customer 3 was a foreign PEP: see paragraphs 118 and 663;

e. between 30 October 2016 and 5 March 2020, Crown Melbourne had given the AUSTRAC CEO 80 SMRs in respect of Customer 3 and the Meg-Star junket;

f. by no later than December 2020, turnover for the Meg-Star junket had exceeded $10,000,000,000 at Crown Melbourne and $442,000,000 at Crown Perth;

g. Customer 3 was known at all times to be connected to Customer 1 in respect of whom Crown Melbourne and Crown Perth had formed suspicions;

h. designated services provided to Customer 3 lacked transparency as the services were provided through the channel of junket programs: see paragraph 477(e);

i. persons associated with the Meg-Star junket, including key players and junket representatives, transacted using large amounts of cash and cash that appeared suspicious, including large volumes of cash in small notes bundled in clear plastic bags which had writing on the side: see paragraphs 450, 451, 452 and 491;

j. Customer 26 was a junket representative of the Meg-Star junket. Customer 26 was a person who posed higher ML/TF risks to Crown Melbourne and Crown Perth for reasons including, among others, that Customer 26 was the owner of a brothel that had been linked to organised crime and other serious criminal activity.

k. multiple key players in the Meg-Star junkets were likely to be foreign PEPs;

l. multiple key players in the Meg-Star junkets were likely to be involved in serious criminal activity;

m. designated services provided to Customer 3 regularly involved large transfers to and from third parties, including to and from other junket representatives of other junket operators, key players and unknown third parties: see paragraph 456ff;

n. funds received for Customer 3 from unknown third parties included transactions related to debt settlement or offsets where the third party was not related to the Meg-Star junket;

o. designated services provided to Customer 3 involved large cross-border movements of funds, including through the Southbank and Riverbank accounts: see paragraph 239;

p. large values were transferred to and from Customer 3's bank accounts and his DAB account, and to and from other customers' DAB accounts, involving the provision by Crown Melbourne of designated services within the meaning of items 31 and 32, table 1, s6 of the Act: see paragraphs 411ff and 492;

q. at various times, Customer 3 was provided with significant amounts of credit upon request, up to limits of $100,000,000 which was reapproved on a regular basis: see paragraphs 280ff and 487;

r. Customer 3 made or received large transfers and unusual requests for transfers to and from other Australian casinos: see paragraphs 398ff and 407ff;

s. at various times, Customer 3 had significant parked or dormant funds in his DAB accounts: see paragraph 252;

t. Customer 3 or his junket representatives engaged in other transactions indicative of ML/TF typologies and vulnerabilities, including structuring and quick turnover of funds (without betting): see paragraph 24;

u. these transactions took place against the background of:

    i. by 2014, Crown Melbourne was aware Meg-Star International Ltd had received investment of about $2,500,000 from a known member of a crime syndicate;

ii. in 2015, Customer 3 engaged in transactions that were indicative of ML/TF typologies involving quick turnover of funds; and

iii. by 1 March 2016 Crown Melbourne had given the AUSTRAC CEO five SMRs regarding Customer 3;

v. by November 2016, media reports named Customer 3 as a person with a relationship with Customer 1;

w. by September 2020, Crown were aware of sources which indicated that the Meg-Star junket was modelled off the Suncity junket and that the Meg-Star operations was part of Customer 1's contingency plan in the event that Suncity or Customer 1 encountered difficulties associated with a high public profile or other allegations;

x. by September 2020, Crown were aware of sources which indicated that a patron Person 26, in respect of whom Crown Melbourne and Crown Perth had formed suspicions was closely associated with the Meg-Star junket; and

y. by reason of the matters set out at subparagraphs a. to x. above, there were real risks that Customer 3's source of wealth and source of funds were not legitimate.

Monitoring of Customer 3's transactions

813. At no time did Crown Melbourne or Crown Perth appropriately monitor Customer 3's transactions on a risk-basis.

Particulars

Section 36(1)(a), (b) of the Act and rules 15.4 to 15.8 of the Rules.

Crown Melbourne and Crown Perth were unable to monitor the ML/TF risks posed by Customer 3's transactions appropriately because they did not make and keep appropriate records of designated services provided to junket operators and players: see paragraphs 483ff.

Crown Melbourne and Crown Perth were unable to monitor the ML/TF risks posed by transactions associated with the Meg-Star junket, including transactions by his junket representatives and key players on his junkets, because they did not make and keep appropriate records of designated services provided: see paragraphs 483ff.

Crown Melbourne and Crown Perth did not apply appropriate risk-based transaction monitoring to designated services provided to Customer 3: see paragraphs 590ff and 629 to 642 (designated services) and 643 to 649 (transactions facilitated through junkets).

Customer 3's transactions involved repeated transactions indicative of ML/TF typologies and vulnerabilities that were not detected. Had appropriate risk-based transaction monitoring been applied, these transactions could have been identified earlier: see paragraphs 686 and 687.

Transactions indicative of ML/TF typologies – quick turnover of funds

Transactions involving Customer 3 were identified as indicative of the ML/TF typology of quick turnover of funds (with no betting) by an independent auditor in 2021.

Between 29 July 2017 and 20 March 2020, Customer 3 engaged in transactions on at least 16 occasions which totalled deposits of $3,672,946 and withdrawals of $6,996,471:

- on 29 July 2017, a deposit of $207,556 by telegraphic transfer followed by a withdrawal of $50,000 in cash on the same day;
- on 30 July 2017, a deposit of $30,000 by telegraphic transfer followed by four withdrawals of $95,190, $19,525, $4,000 and $10,000 in cash on the same day and a further withdrawal of $22,585 in cash on the following day;
- on 19 March 2018, a deposit of $20,000 in cash followed by a withdrawal of $200,000 by telegraphic transfer. On 21 March 2018, a further withdrawal of $135,382 by telegraphic transfer;
- on 1 May 2018, a deposit of $600,486 in cash followed by a withdrawal of $500,000 by telegraphic transfer on the following day;
- on 23 May 2018, a deposit of $100,000 by telegraphic transfer followed by a withdrawal of $100,000 in cash on the same day;
- on 1 October 2018, a deposit of $78,000 in cash followed by a withdrawal of $939,600 by telegraphic transfer and $100,000 in cash on the same day;
- on 13 November 2018, a deposit of $100,000 by telegraphic transfer followed by two withdrawals of $850,000 and $536,185 by telegraphic transfer and $195,000 and $25 in cash and two deposits of $536,185 and $50,000 by telegraphic transfer and three deposits of $100,000, $30,000 and $600 in cash on the following day;
- on 7 February 2019, a deposit of $178,000 by telegraphic transfer and $800 in cash followed by two withdrawals of $200,000 and $800 in cash on the same day;
- on 1 March 2019, a deposit of $73,362 in cash followed by two withdrawals of $100,000 and $5,585 in cash and $70,000 by telegraphic transfer on the same day;
- on 6 March 2019, a deposit of $344,157 by telegraphic transfer followed by a withdrawal of $344,157 by telegraphic transfer on the same day. On 7 March 2019, a withdrawal of $344,157 by telegraphic transfer followed by a further withdrawal of $8,930 by telegraphic transfer on the following day;

- on 2 May 2019, a deposit of $20,000 by telegraphic transfer and $5,800 by cash followed by a withdrawal of $5,906 by telegraphic transfer and $400,000 and $50,106 in cash on the same day;
- on 20 August 2019, a deposit of $500,000 by telegraphic transfer followed by two withdrawals of $409,018 by telegraphic transfer on the same day and a withdrawal of $45,000 and $5,000, $3,000 and $1,800 in cash on the following day;
- on 11 October 2019, a deposit of $100,000 by telegraphic transfer followed by five withdrawals of $40,000, $19,400, $11,200, $10,000 and $500 in cash on the same day;
- on 9 January 2020, a deposit of $100,000 by telegraphic transfer followed by a withdrawal of $301,750 in cash on the same day;
- on 1 March 2020, a deposit of $88,000 in cash followed by a withdrawal of $185,000 by telegraphic transfer on the same day. On 2 March 2020, six withdrawals of $50,500, $9,080, $8,900, $4,500, $4,500 and $200 in cash followed by a further withdrawal of $200,000 in cash the following day; and
- on 19 March 2020, a deposit of $410,000 by telegraphic transfer followed by a withdrawal of $409,990 by telegraphic transfer on the same day.

Transactions indicative of ML/TF typologies – junket operator transactions

Customer 3 engaged in transactions that were identified by an independent auditor in 2021 as indicative of ML/TF typologies involving transactions to third parties who were key players on the Meg-Star junket but where the beneficiary name is different to their key player name and the transaction date was not within the key player's program period.

Transactions indicative of ML/TF typologies – parked funds

Customer 3 engaged in transactions that were identified by an independent auditor in 2021 as indicative of ML/TF typologies involving parked funds of $5,816,626 in one of his safekeeping accounts since 20 July 2020 and $129,998 in a second safekeeping account since 20 July 2020.

Transactions indicative of ML/TF typologies – structuring

Customer 3 engaged in transactions that were identified by an independent auditor in 2021 as indicative of ML/TF typologies involving structuring in respect of at least three of his PIDs at each of Crown Melbourne and Crown Perth.

Other details

The independent auditor also identified that:

- Customer 3 had made 43 payments to 27 unique third parties, to a total value of $29,092,649;

- Customer 3 had sent at least one telegraphic transfer to a Crown patron who was involved in other criminal activity;
- adverse media had been found in respect of Customer 3 relating to money laundering, links to organised crime, illegal gambling or extortion; and
- adverse media had been found in respect of the Meg-Star junket.

Ongoing customer due diligence

814. On and from 1 March 2016, on multiple occasions, the provision of designated services to Customer 3 raised red flags reflective of higher ML/TF risks as a result of Customer 3's frequent, large transactions with a number of third parties included repeated transactions with persons who were not key players in the Meg-Star junket:

Particulars

See paragraph 456ff.

Third party transactions in 2017

On 22 September 2017, Customer 3 instructed Crown Melbourne to send two telegraphic transfers from his account totalling $736,921. The funds were sent to two Australian casinos to be redeemed by a third party who was not a key player under any recent Meg-Star junket: SMR dated 22 September 2017.

On 17 October 2017, Customer 3 instructed Crown Melbourne to send a telegraphic transfer of $490,000 to a key player who was not noted as experiencing a win or loss under any recent junket program: SMR dated 17 October 2017.

On 18 October 2017, Customer 3 instructed Crown Melbourne to send a telegraphic transfer of $60,000 to a third party who was not listed as a key player under any recent junket program: SMR dated 18 October 2017.

On 28 November 2017, Customer 3 received a telegraphic transfer of $50,000 at Crown Melbourne from a third party who was not listed as a key player under any recent junket program: SMR dated 28 November 2017.

On 27 December 2017, Customer 3 received a telegraphic transfer of $1,000,000 at Crown Melbourne from a company account (Company 1): SMR dated 29 December 2017. As pleaded at paragraph 844 below, this company was part of a network of individuals, company accounts and related entities that cumulatively transferred $150,338,386 to Customer 4.

Third party transactions in 2018

On 15 February 2018, Customer 3 received $1,000,000 from a third party into a Southbank account.

On 22 February 2018, Customer 3 received $2,000,000 from a third party and $50,000 from another third party, Person 49, into a

Southbank account, neither of whom were listed as key players on the Meg-Star junket.

On 22 February 2018, Customer 3 received a telegraphic transfer of $38,554.65 at Crown Melbourne from a third party who was not listed as a key player under any recent Meg-Star junket: SMR dated 22 February 2018.

On 28 February 2018, Customer 3 instructed Crown Melbourne to send a telegraphic transfer of $418,137 to a third party who was not listed as a key player under any recent Meg-Star junket: SMR dated 28 February 2018.

On 6 March 2018, Customer 3 instructed Crown Melbourne to send a telegraphic transfer of $300,000 to a company account which appears to belong to an Australian real estate business: SMR dated 6 March 2018.

On 28 March 2018, Customer 3 instructed Crown Melbourne to send a telegraphic transfer of $180,000 to a third party who was not listed as a key player under any recent Meg-Star junket: SMR dated 28 March 2018.

On 22 May 2018, Customer 3 received a telegraphic transfer of $300,000 at Crown Melbourne from an unknown third party: SMR dated 22 May 2018.

On 6 July 2018, a Crown Perth patron withdrew $160,000 from his Crown Perth DAB account and directed the funds to Customer 3's Crown Perth DAB account. Neither the Crown Perth patron nor Customer 3 had any recent recorded gaming activity. The Crown Perth patron was not listed as a key player under the Meg-Star junket. On 9 July 2018, Customer 3 sent the funds by telegraphic transfer to Crown Melbourne in his favour: SMR dated 10 July 2018. The purpose of the transfer was determined to be for the repayment of a debt owed by the Crown Perth patron to the international junket operator Meg-Star for a junket operated in a foreign country.

On 16 August 2018 and 18 August 2018, Customer 3 received a telegraphic transfer of $414,637 and $181,568 at Crown Melbourne from a third party, Person 49, who was not listed as a key player under any recent Meg-Star junket: SMRs dated 17 August 2018 and 20 August 2018.

On 21 September 2018, Customer 3 received two telegraphic transfers of HKD1,000,000 each at Crown Melbourne from a third party who was not listed as a key player under any recent Meg-Star junket: SMR dated 21 September 2018.

On 26 October 2018, Customer 3 instructed Crown Melbourne to send a telegraphic transfer of $2,000,000 to a third party company account for further credit of a third party who was an agent of a junket group in Cairns: SMR dated 30 October 2018.

On 13 November 2018, 14 November 2018, 15 November 2018 and 18 November 2018, Customer 3 received telegraphic transfers of $100,000, $50,000, $100,000 and $100,000 at Crown Melbourne from a third party, Person 46, who was not listed as a key player under any recent Meg-Star junket: SMRs dated 14 November 2018, 15 November 2018, 16 November 2018 18 November 2018.

On 11 December 2018, Customer 3 received $199,990 from a company account into a Riverbank account.

Third party transactions in 2019

On 5 February 2019, Customer 3 received a telegraphic transfer of $178,000 at Crown Melbourne from a third party who was not listed as a key player under any recent Meg-Star junket: SMR dated 6 February 2019.

On 21 February 2019, Crown receive an international funds transfer of $170,000 for the benefit of Customer 3 from a third party.

On 12 February 2019, 5 March 2019 and 23 March 2019, Customer 3 received three telegraphic transfers of $190,000, $500,000 and $200,000 at Crown Melbourne from a third party who Crown Melbourne understood was likely to be a junket representative of another junket but was also affiliated with the Meg-Star junket: SMRs dated 13 February 2019, 6 March 2019, 13 March 2019.

On 23 March 2019, Customer 3 received a telegraphic transfer of $20,000 at Crown Melbourne from a third party who was not listed as a key player under any recent Meg-Star junket: SMR dated 25 March 2019.

On 1 April 2019, Customer 3 received $20,000 and $76,166.84 from a third party, Person 35, into a Southbank account.

On 28 April 2019, Customer 3 instructed Crown Melbourne to send a telegraphic transfer of $132,000 to a third party who was an agent of a junket group in Cairns: SMR dated 29 April 2019.

On 4 June 2019, Customer 3 received an international telegraphic transfer of $300,000 into his Crown Perth DAB account from a Crown Perth patron. Customer 3 used the funds to repay a debt he owed at Crown Perth. The Crown Perth patron, who was not a key player under the Meg-Star junket, was considered to be a business partner of a key player under the Meg-Star junket who had recorded a loss during his last Meg-Star junket program. Customer 3 had also received a deposit of $200,000 from that key player on the same day. Customer 3 signed a requisition to release deposited funds at the Cage: SMR dated 11 June 2019.

On 11 June 2019, 12 June 2019 and 13 June 2019, Customer 3 received six telegraphic transfers totalling $42,000 at Crown Melbourne from a third party who was not listed as a key player under any recent Meg-Star junket: SMR dated 12 June 2019, 13 June 2019, and 14 June 2019.

On 1 July 2019, Customer 3 received two telegraphic transfers of $10,000 each at Crown Melbourne from a third party and $30,000 from another third party, neither of whom were listed as key players under any recent Meg-Star junket: SMR dated 2 July 2019.

On 2 July 2019 and 3 July 2019, Customer 3 received two telegraphic transfers of $20,000 and $10,000 at Crown Melbourne from a third party who was not listed as a key player under any recent Meg-Star junket: SMR dated 3 July 2019, 4 July 2019.

On 23 July 2019, Customer 3 received a telegraphic transfer of $20,000 at Crown Melbourne from a third party and a telegraphic transfer of $30,000 from another third party neither of whom were listed as key players under any recent Meg-Star junket: SMR dated 24 July 2019.

On 25 July 2019, Customer 3 received a telegraphic transfer of $30,000 at Crown Melbourne from a third party who was not listed as a key player under any recent Meg-Star junket: SMR dated 26 July 2019.

On 29 July 2019, Customer 3 received a telegraphic transfer of $500,000 at Crown Melbourne from a third party through a Southbank account who was not listed as a key player under any recent Meg-Star junket: SMR dated 30 July 2019.

On 2 October 2019, Customer 3 received a telegraphic transfer of $300,000 at Crown Melbourne from a third party who was not listed as a key player under any recent Meg-Star junket: SMR dated 3 October 2019.

On 6 November 2019, Customer 3 received a telegraphic transfer of $200,000 at Crown Melbourne from a third party who was not listed as a key player under any recent Meg-Star junket: SMR dated 8 November 2019.

On 25 November 2019, Customer 3 received a telegraphic transfer of $250,000 at Crown Melbourne from a third party (Customer 40) who was not listed as a key player under any recent Meg-Star junket: SMR dated 26 July 2019.

On 2 December 2019, Customer 3 received a telegraphic transfer of $90,000 at Crown Melbourne from a third party who was not listed as a key player under any recent Meg-Star junket: SMR dated 3 December 2019.

On 20 December 2019, Customer 3 received a telegraphic transfer of $150,000 at Crown Melbourne from a third party who was not listed as a key player under any recent Meg-Star junket: SMR dated 23 December 2019.

On 27 December 2019, Customer 3 received a telegraphic transfer of $365,000 at Crown Melbourne from a third party who was not listed as a key player under any recent Meg-Star junket: SMR dated 30 December 2019.

Third party transactions in 2020

On 7 January 2020, Customer 3 received a telegraphic transfer of $119,420 at Crown Melbourne from a third party who was not listed as a key player under any recent Meg-Star junket: SMR dated 9 January 2020.

On 16 January 2020, Customer 3 received a telegraphic transfer of $150,000 at Crown Melbourne from a third party who was not listed as a key player under any recent Meg-Star junket: SMR dated 17 January 2020.

815. On and from 1 March 2016, on multiple occasions, the provision of designated services to Customer 3 raised red flags reflective of higher ML/TF risks as a result of complex, unusual large transactions and unusual patterns of transactions involving Customer 3 which had no apparent economic or visible lawful purpose.

Particulars

See paragraphs 420ff, 450, 451 and 491.

Unusual transactions and patterns of transactions in 2016

In 2016, Crown Melbourne recorded Customer 3's individual rated gaming activity as cumulative loss of $327,748.

Unusual transactions and patterns of transactions in 2017

In 2017, Crown Melbourne recorded Customer 3's individual rated gaming activity as cumulative win of $397,139.

On 8 March 2017, Customer 3 transferred $50,000 from his Crown Melbourne DAB account to another Crown Melbourne patron despite the patron not being a key player in any of Customer 3's recent junket programs: SMR dated 8 March 2017.

On 22 September 2017 alone, Customer 3 had a turnover of $3,123,000 and a win of $142,090.

Unusual transactions and patterns of transactions in 2018

On 21 March 2018, Customer 3 withdrew $37,080 from his Crown Perth DAB account and deposited the sum into the DAB account of another Crown Perth patron. However, the Crown Perth patron had no recorded activity as a key player in the Meg-Star junket: SMR dated 21 March 2018.

On 3 April 2018, a Crown Melbourne customer exchanged $75,000 in commission-based chips for cash which was not supported by rated gaming activity. Another Crown Melbourne customer then deposited the same cash while Customer 3 stood behind him. Neither Crown Melbourne customers were noted as key players under a Meg-Star junket program: SMR dated 3 April 2018.

On 16 April 2018, a Suncity junket representative brought two Meg-Star junket key players to the Suncity cash administration desk (see paragraph . The key players presented three bundles of cash

comprised of $100 notes totalling approximately $34,000. While the funds were being counted, the Suncity junket representative was in discussions with a Meg-Star junket representative to request the transfer of the key players from the Meg-Star junket to the Suncity junket. The request was denied and the funds returned to the customers: SMR dated 16 April 2018.

On 3 May 2018, a Meg-Star junket representative requested a $500,000 transfer to a Crown Melbourne patron, Person 31, who was not a key player in the Meg-Star junket. The request was denied because the key player was a domestic patron. A number of complex transactions then occurred which ultimately allowed the Crown Melbourne patron to repay an outstanding CCF balance, including the issuing of cash chips to a junket player while they were still key players on the Meg-Star junket, telegraphic transfers to Meg-Star key players which did not match rated gaming activity, obtaining funds to redeem a CCF from another key player in the Meg-Star junket and transfers from a DAB account to persons who were not key players in the Meg-Star junket: SMR dated 4 May 2018.

On 8 May 2018, Customer 3 sent a telegraphic transfer of $36,000,000 to his Crown Melbourne DAB.

On 17 May 2018, a Meg-Star junket representative deposited $800,000 in cash, comprising bundled $50 notes, into the Meg-Star account. The cash belonged to a Crown Melbourne patron, Person 11, who was not a key player in the Meg-Star junket: SMR dated 17 May 2018.

On 27 July 2018, a Meg-Star junket representative deposited $300,000 in cash, comprising bundles of cash in clear plastic bags on which was written the date 24 July 2018, into Customer 3's DAB account. The junket representative was unwilling to answer questions relating to the source of the funds. Crown Melbourne later determined the funds to belong to a Crown Melbourne patron, Person 11, who was not a key player in, or junket representative of, the Meg-Star junket. The funds were presented on behalf of a key player in the Meg-Star junket, but the identity of the key player was not disclosed: SMR dated 27 July 2018.

On 3 August 2018, a Meg-Star junket representative presented a $270,000 receipt advising of a transfer to Crown Melbourne's bank account from a Crown Melbourne patron who was a junket representative of another junket operator, Person 22. The transfer was for a Meg-Star key player: SMR dated 3 August 2018.

Unusual transactions and patterns of transactions in 2019

On 23 February 2019, a Crown Perth patron withdrew $363,636, corresponding to his junket winnings, from his Crown Perth DAB account and directed the funds to Customer 3's Crown Perth DAB account. The Crown Perth patron refused to provide a reason for the transfer when asked. Customer 3 and the Crown Perth patron were

considered by Crown Perth to be business partners. On 26 February 2019, Customer 3 signed an authority to disperse form authorising the balance of his DAB account, being $563,636, to be sent by telegraphic transfer to Crown Melbourne in his favour: SMR dated 27 February 2019.

On 9 April 2019, Customer 3's Crown Melbourne DAB account received a telegraphic transfer of $600,000 from a third party (Customer 40) and $89,000 from another third party, Person 45, who were listed as key players under recent Meg-Star junkets but the transactions were not supported by rated gaming activity: SMR dated 10 April 2019.

On 17 and 19 July 2019, Customer 3 received several transactions from a key player under the Meg-Star junket that did not correspond with any recorded junket play: SMR dated 24 July 2019.

On 19 August 2019, Customer 3's Crown Melbourne DAB account received a telegraphic transfer of $500,000 from a third party who was listed as a key player under a recent Meg-Star junket but was showing a loss of $6,930 at the time: SMR dated 20 August 2019.

On 13 November 2019, Customer 1 received two telegraphic transfers of $100,000 each from a third party, Person 20, who was a key player under Meg-Star junket and not under the Suncity junket: SMR dated 13 November 2019.

In FY2019, Customer 3 received $19,885,502 into his Crown Melbourne DAB account, including $523,133 in three transactions from Crown Perth, $1,500,000 in one transaction from an Australian casino, $9,831,811 in two transactions from Meg-Star International Ltd and $1,794,695 in 31 transactions from Customer 3's personal account.

In FY2019, Customer 3 transferred out $14,606,950.20 from his Crown Melbourne DAB, including $1,057,416 to Crown Perth, $7,939,600 to Meg-Star International Ltd and $2,744,934.20 to an Australian casino.

On 11 December 2019, a Meg-Star junket representative deposited $150,000 in cash into Customer 3's Crown Melbourne DAB. The junket representative indicated that the funds were from a Crown Melbourne patron who had previously been a key player in the Meg-Star junket, however he was not a key player at that time: SMR dated 11 December 2019.

Unusual transactions and patterns of transactions in 2020

On 15 February 2020, a Crown Perth customer directed $100,000 to Customer 3's DAB account for the purpose of front money for another Crown Perth customer who was a key player in, and junket representative of, the Meg-Star junket. The funds were fully utilised for gaming purposes. The two Crown Perth customers were known to be business partners

On 2 March 2020, a Meg-Star junket representative deposited $100,000 in cash into Customer 3's Crown Melbourne DAB account. The funds were from a Crown Melbourne patron, who was not a key player in any recent Meg-Star junket: SMR dated 2 March 2020.

On 5 March 2020, a Meg-Star junket representative and a Meg-Star key player presented $100,000 in gaming chips for exchange to cash. The key player had no rated gaming activity to support the transaction. The junket representative then withdrew $100,000 from the DAB account instead and handed the cash to the key player, who in turn handed the chips to the junket representative: SMR dated 5 March 2020.

On 23 March 2020, Customer 3 had a Crown Melbourne debt of $27,072,267. By 10 December 2020, that debt remained unpaid.

On 14 April 2020, Customer 3 had a Crown Perth debt of $33,000,000 and $30,343,084 in his DAB account. By 10 December 2020, that debt remained unpaid.

816. On and from 1 March 2016, on multiple occasions, the provision of designated services to Customer 3 raised red flags reflective of higher ML/TF risks as a result of the Meg-Star junket's activity.

Particulars

See paragraph 477.

Meg-Star credit limit

On 7 April 2016, the Meg-Star credit limit was increased to $20,000,000.

On 29 April 2018, the Meg-Star junket credit limit was increased to $100,000,000 on a 60/40 basis such that Crown had a net exposure of $40,000,000.

Meg-Star turnover at Crown Melbourne

In FY2016 the Crown Melbourne Meg-Star junket had a turnover of $104,227,800 with a cumulative loss of $887,732.

In FY2017 the Crown Melbourne Meg-Star junket had a turnover of $531,299,000 with a cumulative loss of $11,360,820.

In FY2018 the Crown Melbourne Meg-Star junket had a turnover of $4,091,818,098 with a cumulative loss of $46,615,998.

Between 1 July 2018 and 1 March 2019, Customer 3 ran junket programs at Crown Melbourne for 181 unique key players with estimated total turnover $2,260,428,216.92, being over 13.5% of the total junket turnover at Crown Melbourne during that period, and estimated cumulative loss of $8,552,445.49.

Between 1 April 2019 and 1 May 2019, Customer 3 ran junket programs at Crown Melbourne for 20 unique key players with

estimated total turnover $82,411,266.99 and estimated cumulative loss of $3,842,576.43.

In FY2019 the Crown Melbourne Meg-Star junket had a turnover of $3,026,381,929 with a cumulative loss of $9,471,517.

In FY2020 (to 1 October 2019) the Crown Melbourne Meg-Star junket had a turnover of $523,527,332 with a cumulative loss of $34,269,550.

By 10 December 2020, the Meg-Star junket had an approximate turnover at Crown Melbourne of AUD10,000,000,000 and a loss of $60,000,000.

By 1 October 2019, the Meg-Star junket was paid a cumulative commission by Crown Melbourne of $67,943,227.

Meg-Star turnover at Crown Perth

In FY2017, the Crown Perth Meg-Star junket had a turnover of $10,286,116 with a cumulative win of $229,558.

In FY2018, the Crown Perth Meg-Star junket had a turnover of $164,399,300 with a cumulative loss of $4,681,725.

In FY2019 (to 24 March 2019), the Crown Perth Meg-Star junket had a turnover of $126,604,344 and a cumulative win of $4,179,482.

By 10 December 2020, the Meg-Star junket had a turnover at Crown Perth of $442,000,000 and a loss of $11,000,000.

By 24 March 2019, the Meg-Star junket was paid a cumulative commission by Crown Melbourne of $1,103,235.

Other Meg-Star red flags

In at least March 2018, Customer 26 acted as the junket representative of the Meg-Star junket. As pleaded at paragraphs 1320, 1322, 1324, 1325 and 1326 below, Customer 26 was a person who posed higher ML/TF risks to Crown Melbourne and Crown Perth including, among other reasons, that Customer 26 was the owner of a brothel that had been linked to organised crime and other serious criminal activity.

817. Between July 2019 and March 2020, Crown Melbourne became aware of articles published between 2017 and 2020 detailing Customer 3's involvement in Meg-Star International Ltd and his affiliation with Customer 1.

Particulars

In July 2019, Crown Melbourne senior management conducted an open source media search in respect of Customer 3. One of the resulting articles was published in November 2016 and identified a relationship between Customer 3 and Customer 1.

In March 2020, Crown saved multiple articles published between February 2018 and January 2020. The articles described Meg-Star International Ltd as a gaming conglomerate with broad business

interests and reported the launch of new gaming rooms by Meg-Star International Ltd including at Crown Melbourne in April 2018.

818. At no time did Crown Melbourne or Crown Perth undertake appropriate risk-based customer due diligence with respect to Customer 3 with a view to identifying, mitigating and managing the ML/TF risks posed by the provision of designated services on and from 1 March 2016.

a. At no time did Crown Melbourne or Crown Perth take appropriate steps to understand Customer 3's source of wealth/funds was legitimate. To the extent that Crown Melbourne and Crown Perth took steps to understand Customer 3's source of wealth/funds, this was for the purpose of approving credit applications for the Meg-Star junket, not for the purpose of assessing the ML/TF risks associated with Customer 3's source of wealth/funds.

b. At no time did Crown Melbourne or Crown Perth take appropriate steps to identify or analyse the ML/TF risks of Customer 3's transactions or to consider whether they had a lawful purpose.

c. At no time did Crown Melbourne give appropriate consideration to whether large and high risk transactions should be processed.

d. On two occasions, Crown Perth gave consideration to whether large and high risk transactions should be processed. However, on both occasions the transactions were processed despite the higher ML/TF risk they posed.

e. On each occasion prior to January 2021 that senior management considered whether to continue the business relationship with Customer 3, senior management failed to give adequate consideration to whether the ML/TF risks posed by Customer 3 were within Crown Melbourne and Crown Perth's risk appetite.

Particulars

Section 36(1)(a) of the Act.

Due diligence searches between 2016 and 2019

Between March 2016 and March 2020 Crown conducted a number of searches in respect of Customer 3 on open sources and subscription databases which identified:

- information about Meg-Star International Ltd and Customer 3's relationship to it as a member and administrator;
- Customer 3 was a known associate of Customer 1;
- Customer 3's high net worth and his affiliation with Meg-Star International Ltd; and
- Customer 3 to be a foreign PEP and an advisor of a foreign gaming body.

At no point, as a result of these searches, did Crown Melbourne appropriately consider the ML/TF risks of the source of Customer 3's wealth/funds or whether an ongoing business relationship with Customer 3 was within its risk appetite.

Due diligence searches conducted in 2020

In 2020, Crown conducted more extensive due diligence searches using open sources and subscription databases in respect of Customer 3 and the Meg-Star junket. These searches identified that a number of Meg-Star's known associates had been charged with or accused of crimes including embezzlement, bribery in a foreign country and organising prostitution.

At no point, as a result of these searches, did Crown Melbourne or Crown Perth appropriately consider the ML/TF risks of the source of Customer 3's wealth/funds or whether an ongoing business relationship with Customer 3 was within its risk appetite.

Credit reports

On various occasions between 3 March 2016 and 8 May 2019, Crown Perth prepared a credit profile for the purpose of extending the Meg-Star junket a line of credit.

On various occasions between 2 March 2016 and 4 October 2019, Crown Melbourne prepared a credit profile and obtained a central credit check in respect of Customer 3 for the purpose of extending the Meg-Star junket a line of credit, which varied between $2,000,000 and $100,000,000 throughout that period.

Crown Melbourne and Crown Perth did not appropriately consider the ML/TF risks in respect of these credit profiles or when extending credit to Customer 3.

Junket reviews

In May 2017, March 2018, December 2018 and March 2020 Crown prepared junket profiles in respect of the Meg-Star junket. The profiles:

- set out Customer 3's credit limit and turnover and Crown Melbourne and Crown Perth;
- set out Customer 3's junket and individual credit lines at other casinos; and
- summarised searches conducted in respect of Customer 3 including wealth reports, risk intelligence reports, risk intelligence searches, company searches and property searches.

Each junket profile recommended that Crown continue to conduct business with Customer 3.

In December 2020, Crown prepared a junket profile in respect of the Meg-Star junket. In addition to the information contained in previous profiles, the December 2020 profile included:

- Customer 3's debt history at Crown Perth and Crown Melbourne.
- that Customer 3 had last visited Crown Melbourne on 28 November 2019;

- that 86 SMRs had been given to the AUSTRAC CEO in respect of Customer 3 between 2015 and 2020 which predominantly reflected significant losses by key players, third party deposits and withdrawals; and
- that no law enforcement enquiries or production orders had been made in respect of Customer 3.

Crown Melbourne did not appropriately consider the ML/TF risks of the source of Customer 3's wealth/funds in any of the junket profiles.

External due diligence report obtained in 2020

On 18 March 2019, Crown carried out due diligence in respect of Customer 3 as a part of its efforts to review all junkets operating at that time. The review included a customer's Crown history, their history with other casinos, and information available through database and open source searches. No action appears to have been taken in respect of Customer 3 as a result of the review.

On 12 September 2020, Crown was issued the findings of an external due diligence report which investigated several customers, including Customer 3. The external provider was engaged to uncover actual background, business activities, reputation (including corruption and bribery-related matters), regulatory and compliance issues, and any significant 'red flag issues' that could affect Crown's evaluation of them, including any litigation or involvement in government investigations. The report included, among other things, the following information:

- Customer 3 was a foreign PEP by association;
- Customer 3 had four registered addresses in two foreign countries;
- Customer 3 was the founder and chairman of Meg-Star International Ltd. Sources indicated that junket operation was the major service provided by the diversified entertainment group;
- Meg-Star International Ltd operated eight VIP clubs in a foreign country; and
- Customer 3 was an advisor of a foreign gaming body.

At no point, as a result of this report, did Crown Melbourne or Crown Perth appropriately consider the ML/TF risks of the source of Customer 3's wealth/funds or whether an ongoing business relationship with Customer 3 was within its ML/TF risk appetite.

Consideration of suspicious transactions

Of the large and suspicious transactions involving Customer 3 pleaded at paragraph 814 and 815, it was only on the following occasions that Crown Perth considered the purpose of those transactions. On no occasion did Crown Perth reject the processing of any transactions:

- on 9 July 2018, an AML Legal Officer emailed the Crown Perth VIP International Business Operations team to determine the relationship between a Crown Perth patron who had deposited funds in Customer 3's DAB account. The customer was a key player in an international Meg-Star junket;
- on 27 February 2019, an AML Legal Officer emailed the Crown Perth VIP International Business Operations team to determine the relationship between a Crown Perth patron who had deposited funds in Customer 3's DAB account. The customer was considered by Crown Perth to be a business partner of Customer 3.

Crown Melbourne gave no consideration at any time to whether large and high risk transactions should be processed.

Senior management engagement

On 25 January 2017, there was a Crown Melbourne VIP Operations meeting. The minutes included a junket due diligence profile summary for Customer 3. There is no evidence that the attendees at the meeting considered whether continuing a business relationship with Customer 3 was in Crown Melbourne's ML/TF risk appetite.

On 5 April 2017, following receipt of a due diligence search that identified Customer 3 as a foreign PEP , the Executive General Manager (Legal & Regulatory Services) approved Crown Melbourne continuing a business relationship with Customer 3.

On 28 May 2019, the Group General Manager – AML reviewed Crown's files relating to the Meg-Star junket. There is no evidence any further action was taken, or that the Group General Manager – AML considered whether continuing a business relationship with Customer 3 was in Crown Perth's risk appetite.

On 17 July 2019, a Crown Perth AML review of the Meg-Star junket was conducted because there had been significant cash transactions noted.

On 20 January 2021, the Crown Resorts POI Committee considered Customer 3, who had come to the Committee's attention through the ILGA inquiry and agreed to issue a WOL/NRL with respect to Customer 3.

On 22 January 2021, the WOL took effect at Crown Melbourne.

On 29 January 2021, the NRL took effect at Crown Perth.

Prior to January 2021, none of these steps set out above were proportionate to the ML/TF risks reasonably posed by Customer 3 on and from 1 March 2016.

Enhanced customer due diligence

819. Having formed a suspicion for the purposes of s41 of the Act, Crown Melbourne gave the AUSTRAC CEO SMRs with respect to Customer 3 on 80 occasions: Schedule 3.3.

Particulars

The SMRs reported:

- significant individual and junket losses noted for key players in the Meg-Star junket;
- cash deposits from a third party not noted as a key player on the Meg-Star junket;
- large deposits at the Suncity cash administration desk by key players in the Meg-Star junket;
- funds shared between key players in the Meg-Star junket and third parties;
- telegraphic transfers to and from third parties who were not key players in the Meg-Star junket and company accounts;
- telegraphic transfers to third parties and key players in the Meg-Star junket with no play to support the transaction; and
- the amount of cash key players in the Meg-Star Junket were prepared to carry.

820. Having formed a suspicion for the purposes of s41 of the Act, Crown Perth gave the AUSTRAC CEO SMRs with respect to Customer 3 on:

a. 21 March 2018;

b. 10 July 2018;

c. 27 February 2019;

d. 21 March 2019;

e. 11 June 2019;

f. 24 July 2019; and

g. 21 February 2020.

Particulars

The SMRs reported:

- transactions to Customer 3's Crown Perth DAB account from persons who were not key players under the junket;
- transfers to key players under the Meg-Star junket in circumstances where there was no corresponding gaming activity;
- the transfer of key player winnings to the Customer 3's DAB account for no apparent reason; and
- transfers of funds between junket operators.

821. On each occasion that Crown Melbourne and Crown Perth formed a suspicion with respect to Customer 3 for the purposes of s41 of the Act, it was required to apply its ECDD program to Customer 3.

Particulars

Rule 15.9(3) of the Rules.

822. Crown Melbourne and Crown Perth did not carry out appropriate risk-based ECDD measures with respect to Customer 3 on each occasion that Crown Melbourne or Crown Perth formed a suspicion with respect to Customer 3 for the purposes of s41 of the Act.

a. With the exception of the SMRs given to the AUSTRAC CEO on 30 December 2019, 9 January 2020, 20 March 2020 and 5 March 2020, there are no records of ECDD being conducted by Crown Melbourne after the SMRs were given between 27 April 2016 and 20 March 2020: see paragraphs 664 and 685.

b. There are no records of ECDD being conducted by Crown Perth following the lodgement of SMRs on 21 March 2018, 10 July 2018, 27 February 2019, 11 June 2019 and 24 July 2019: see paragraphs 664 and 685.

c. Appropriate risk-based steps were not taken to obtain or analyse information about Customer 3's source of wealth/funds in order to understand whether that source was legitimate: see paragraph 667.

d. Appropriate risk-based steps were not taken to analyse and monitor Customer 3's transactions – both past and future – including to understand their economic purpose: see paragraphs 590 and 666.

e. On each occasion prior to January 2021 that senior management considered whether to continue the business relationship with Customer 3, senior management failed to give adequate consideration to whether the ML/TF risks posed by Customer 3 were within Crown Melbourne and Crown Perth's risk appetite: see paragraph 668ff.

Particulars

Rule 15.9(3), 15.10(1)(c), (d), (2), (5) and (6) of the Rules.

Prior to giving the 30 December 2019 and 9 January 2020 SMRs to the AUSTRAC CEO, Crown Melbourne conducted risk intelligence searches in respect of Customer 3 and the persons involved in the transactions the subject of the SMRs which returned no results. However, these steps were not proportionate to the ML/TF risks reasonably posed by Customer 3 as identified in the SMRs given to the AUSTRAC CEO by Crown Melbourne.

In March 2020, after the SMRs were given to the AUSTRAC CEO on 2 March 2020 and 5 March 2020, Crown Melbourne requested that ECDD be conducted in respect of Customer 3. Risk intelligence searches were completed in respect of both Customer 3 and the persons involved in transactions the subject of the SMRs. This appears to have resulted in much of the due diligence conducted in 2020 as pleaded at paragraph 818.

823. At all times from 1 March 2016, Customer 3 was a foreign PEP.

Particulars

Section 36(1)(a) of the Act.

See particulars to paragraph 808.

824. At all times from 1 March 2016, Crown Melbourne and Crown Perth were required to apply its ECDD program to Customer 3.

Particulars

Rule 15.9(2) and 15.11 of the Rules.

See paragraphs 660, 663 and 666.

825. Crown Melbourne and Crown Perth did not carry out appropriate risk-based ECDD measures with respect to Customer 3 on and from 1 March 2016 given his status as a foreign PEP. In particular:

a. Crown Melbourne and Crown Perth did not undertake a detailed analysis of Customer 3's KYC information or analyse the legitimacy of Customer 3's source of wealth/funds.

b. Senior management approval for Crown Melbourne and Crown Perth to continue a business relationship with Customer 3 did not give adequate consideration to the ML/TF risks posed by the customer.

c. Senior management approval for Crown Melbourne or Crown Perth to continue to provide designated services to Customer 3 did not give adequate consideration to the ML/TF risks posed by the customer.

Particulars

Rule 15.10(2), 15.10(6) and 15.11 of the Rules.

See particulars to paragraph 818.

See paragraph 660, 663, 666, 667 and 668.

826. On and from 5 April 2017, Crown Melbourne rated Customer 3 high risk.

Particulars

Crown Melbourne rated Customer 3 high risk on at least various occasions between 5 April 2017 and 16 February 2021: see paragraph 810.

827. On and from 20 January 2021, Crown Perth rated Customer 3 high risk.

Particulars

Crown Perth rated Customer 3 high risk on various occasions between 20 January 2021 and 31 July 2021: see paragraph 811.

828. On each occasion that Crown Melbourne and Crown Perth rated Customer 3 high risk, Crown Melbourne and Crown Perth was required to apply its ECDD program to Customer 3.

Particulars

Rule 15.9(1).

Between 5 April 2017 and 16 February 2021, Crown Melbourne rated Customer 3 high risk on 81 occasions.

Between 20 January 2021 and 31 July 2021, Crown Perth rated Customer 3 high risk on 3 occasions.

See paragraph 661.

829. Crown Melbourne and Crown Perth did not carry out appropriate risk-based ECDD measures with respect to Customer 3 on each occasion that Crown Melbourne and Crown Perth rated Customer 3 high risk.

Particulars

Despite the matters pleaded at paragraphs 807, 808, 812, 813, 814, 815, 816, 817, and 819 other than in March 2020, at no time did Crown Melbourne conduct ECDD following each occasion that it rated Customer 3 high risk.

Despite the matters pleaded at paragraphs 807, 808, 812, 813, 814, 815, 816 and 820, other than in February 2020, at no time did Crown Perth conduct ECDD following each occasion that it rated Customer 3 high risk.

See the particulars to paragraph 818.

See paragraphs 661, 666, 667 and 668.

830. By reason of the matters pleaded from paragraphs 801 to 829, on and from 1 March 2016, Crown Melbourne and Crown Perth:

a. did not monitor Customer 3 in relation to the provision of designated services, with a view to identifying, mitigating and managing the ML/TF risks reasonably faced; and

b. did not do so in accordance with rr15.5 and 15.9 of the Rules.

831. By reason of the matters pleaded at paragraph 830, Crown Melbourne and Crown Perth contravened s36(1) of the Act on and from 1 March 2016 to January 2021 with respect to Customer 3.

Particulars

Section 36(1) of the Act is a civil penalty provision: s36(2) of the Act.

Customer 4

832. Customer 4 has been a customer of Crown Melbourne since 22 May 2008.

833. From at least May 2008, Crown Melbourne provided Customer 4 with designated services within the meaning of table 1 and table 3, s6 of the Act.

834. From at least May 2008, Customer 4 received designated services as a junket operator and as a junket player, facilitated through two different junket operators, at Crown Melbourne.

Particulars to paragraphs 833 and 834

Customer 4 was registered as a junket operator on 22 May 2008 and had four PIDs.

On and from 13 August 2010, Customer 4 signed several NONEGPRAs with Crown. On 3 June 2019, Customer 4 signed a further NONEGPRA with Crown Melbourne and Crown Perth.

On 29 April 2010, Crown Melbourne opened a credit facility account (AUD/HKD) for Customer 4. The credit facility was closed on 23 November 2020.

On 29 April 2013, Crown Melbourne opened a DAB account and safekeeping account (AUD) for Customer 4, which remains open. Crown Melbourne also opened further DAB accounts and safekeeping accounts (AUD and AUD/HKD) for Customer 4 on 4 February 2016, 8 May 2018, 24 November 2019 and 30 April 2020, which all remain open.

Between 23 March 2016 and 23 March 2020, Customer 4 operated 131 junket programs at Crown Melbourne: 53 under one PID, 52 under a second PID, 23 under a third PID and three under a fourth PID. In that period, Customer 4 had 11 junket representatives.

Customer 4 was a key player in his own junket program and in Customer 10's Chinatown junket program.

Between 2010 and 2020, Customer 4's junket at Crown Melbourne had a turnover of $13,657,295,383 and a loss of $248,269,666.

On and from 1 March 2016, Customer 4's highest yearly junket turnover was in 2018 and totalled $4,167,900,329.

On 22 and 23 January 2021, Crown Melbourne applied stop codes in relation to three of Customer 4's four PIDs. However, on 28 June 2021, Customer 4 was able to transfer the balance of his Crown Melbourne DAB, being $7,079,089, to an international bank account in his name.

835. Customer 4 has been a customer of Crown Perth since 6 April 2010.

836. From at least 6 April 2010, Crown Perth provided Customer 4 with designated services within the meaning of table 1 and table 3, s6 of the Act.

837. From at least 6 April 2010, Customer 4 received designated services as a junket operator at Crown Perth.

Particulars to paragraphs 836 and 837

On 6 April 2010, Customer 4's junket was approved to operate at Crown Perth. On and from 13 August 2010, Customer 4 signed several NONEGPRAs with Crown. On 3 June 2019, Customer 4 signed a further NONEGPRA with Crown Melbourne and Crown Perth.

Between 23 June 2016 and 28 February 2020, Customer 4 operated 38 junket programs at Crown Perth: seven under one PID, 27 under a second PID and four under a third PID. In that period, Customer 4 had three junket representatives.

On 6 July 2011, Crown Perth opened a DAB account and safekeeping account (AUD/HKD) for Customer 4, which remains open. Crown Perth also opened further DAB account and safekeeping accounts (AUD/HKD) for Customer 4 on 13 July 2011, 11 August 2016 and 26 September 2019, which remain open.

On 11 July 2016, Crown Perth opened two FAF accounts (AUD/HKD) for Customer 4. The accounts were closed on 20 November 2020.

Between 2011 and 2020, Customer 4's junket at Crown Perth had a turnover of $3,033,089,501 and a loss of $13,552,931.

On and from 1 March 2016, Customer 4's highest yearly junket turnover was in 2018 and totalled $1,641,003,721.

The ML/TF risks posed by Customer 4

838. By 1 March 2016, higher ML/TF risks were indicated by the nature and purpose of Customer 4's business relationship with Crown Melbourne and Crown Perth, the nature of the transactions he had been conducting, together with the suspicions Crown Melbourne and Crown Perth itself had formed with respect to Customer 4.

Particulars

Section 36(1)(a), (b) of the Act and Chapter 15 of the Rules.

Customer 4 was a junket operator and junket player. He received and facilitated the provision of designated services through the channel of junket programs. This channel lacked transparency: see paragraph 477.

Junket activity

Between 28 January 2012 and 14 November 2019, Customer 4 facilitated at least 202 junket programs at Crown Melbourne.

SMRs

Between 3 May 2010 and 29 February 2016, Crown Melbourne gave the AUSTRAC CEO 79 SMRs in respect of Customer 4: Schedule 3.4.1.

The SMRs reported, among other things, the wins/losses of key players in Customer 4's junket including himself, telegraphic transfers received by Customer 4 from key players, third parties (domestic and international) who were not key players and other casinos, telegraphic transfers sent by Customer 4 with no rated play to justify the transfer and other suspicious behaviour of key players in Customer 4's junket.

Collectively, the SMRs given to the AUSTRAC CEO between 1 March 2013 and 29 February 2016 reported total junket wins of $9,635,730 and total junket losses of $45,297,702 over this period. This included total junket wins of $428,135 and total junket losses of $100,000 by Customer 4 personally as a key player in his junket

program: SMRs dated 27 March 2011, 17 October 2011, 6 September 2013.

The SMRs given to the AUSTRAC CEO between 1 March 2013 and 29 February 2016 reported:

- one telegraphic transfer to Customer 4's DAB account from a key player totalling $100,000: SMR dated 22 July 2015;
- one telegraphic transfer to Customer 4's DAB account from a junket representative totalling $400,000: SMR dated 26 April 2012;
- three telegraphic transfer from Customer 4's DAB account to a junket representative totalling $1,530,000: SMRs dated 26 March 2014, 9 May 2014, 15 September 2015;
- 12 telegraphic transfers to Customer 4's DAB account from third party individuals totalling $6,914,847: SMRs dated 8 December 2012, 27 March 2012, 28 February 2013, 19 April 2013, 5 June 2013, 22 August 2014, 3 February 2015, 19 February 2015, 24 March 2015, 7 August 2015, 18 August 2015;
- 14 telegraphic transfers from Customer 4's DAB account to third party individuals totalling $3,265,363: SMRs dated 8 March 2013, 23 September 2013, 13 December 2013, 25 January 2014, 14 April 2014, 18 June 2014, 15 July 2014, 4 September 2014, 3 October 2014, 3 February 2015, 18 February 2015, 10 March 2015, 18 January 2016, 27 February 2016;
- three telegraphic transfers to Customer 4's DAB account from company accounts including Company 6 totalling $1,450,277: SMRs dated 11 July 2011, 15 May 2013, 21 December 2015; and
- three telegraphic transfers from Customer 4's DAB account to company accounts totalling $1,015,983: SMRs dated 8 December 2010, 23 April 2013, 18 July 2014.

The telegraphic transfers included large cross-border movement of funds to third parties and companies unknown to Crown Melbourne.

Large and suspicious third party transactions

By 1 March 2016, Customer 4 was involved in many large cash and telegraphic transactions. In 2015, Customer 4 received by telegraphic transfer approximately $7,652,267 from third parties and sent by telegraphic transfer approximately $1,411,447 to third parties. These included:

- on 3 February 2015 and 17 February 2015, Customer 4 received four telegraphic transfers of $1,000,000 each from a third party;
- on 17 February 2015, Customer 4 received a telegraphic transfer of $1,500,000 with no ordering name listed;

- on 24 March 2015, Customer 4 received a telegraphic transfer of $1,300,000 from a third party;
- on 26 May 2015, Crown Melbourne received into a Southbank account a transfer of $1,000,000 from Company 14 with Customer 4's PID as the reference number;
- on 15 September 2015, Customer 4 sent a telegraphic transfer of $500,000 to a company account; and
- on 21 December 2015 and 18 February 2016, Customer 4 received a telegraphic transfer of $252,277 and $510,347 from Company 6's account.

Junket activity

Customer 4 was a key player on his own junket program at Crown Melbourne in at least March 2011, October 2011 and September 2013.

Between 10 January 2015 and 24 January 2015, Customer 4 attended Crown Melbourne as a key player in Customer 10's Chinatown junket.

Between 2010 and 2015, Customer 4's junket at Crown Melbourne had a turnover of $3,005,469,301 and a loss of $54,280,543.

Between 2011 and 2015, Customer 4's junket at Crown Perth had a turnover of $171,672,675 and a loss of $8,004,570: SMR dated 7 December 2021.

Other red flags

On 28 May 2015, Customer 4's junket representative attempted to deposit $100,000 in cash but declined to complete any paperwork or compliance requirements and presented a loyalty card of a different patron: SMR dated 28 May 2015.

Between 26 March 2014 and 29 February 2016, Customer 4 engaged in transactions indicative of ML/TF typologies involving quick turnover of funds (without betting) on at least four occasions:

- on 26 March 2014, a deposit of $1,300,000 by telegraphic transfer and two deposits of $98,000 and $14,000 in cash were made to Customer 4's DAB account followed by a withdrawal of $200,000 in cash on the same day;
- on 1 June 2015, two deposits of $200,000 and $100,000 were made by telegraphic transfer to Customer 4's DAB account followed by three withdrawals of $200,000, $52,000 and $2,000 in cash on the following day;
- on 31 August 2015, two withdrawals of $300,000 by telegraphic transfer and $20,000 in cash were made from Customer 4's DAB account followed by a deposit of $440,935 on the same day. The following day, four withdrawals of $110,000, $12,900, $5,000 and $5,000 in cash were made from Customer 4's DAB account; and

- on 29 February 2016, four withdrawals of $100,000, $31,000, $10,000 and $2,500 in cash were made from Customer 4's DAB account followed by deposits of $100,000 by telegraphic transfer and $60,000 in cash on the same day.

By 2016, Crown Melbourne were aware that Customer 4's junket operated as a sub-junket of a foreign junket tour operator.

Due diligence

In November 2015, Crown conducted a risk intelligence search in respect of Customer 4.

As at 1 March 2016, despite Customer 4's junket turnover at Crown Melbourne and Crown Perth being a cumulative $3,177,141,976, no other due diligence was recorded in respect of Customer 4.

839. As at 1 March 2016, Customer 4 should have been recognised by Crown Melbourne and Crown Perth as a high risk customer for the reasons pleaded at paragraph 838.

840. At all times on and from 1 March 2016, Customer 4 should have been recognised by Crown Melbourne and Crown Perth as a high risk customer by reason of the matters pleaded at paragraphs 838, 843, 844, 845, 846, 847, 848, 850 and 851.

Particulars

Section 36(1)(a), (b) of the Act and Chapter 15 of the Rules.

841. It was not until 26 August 2021 that Customer 4 was rated high risk by Crown Melbourne.

Particulars

On various occasions between 3 May 2010 and 4 July 2018, Crown Melbourne rated Customer 4's risk as moderate.

On various occasions between 5 July 2018 and 25 August 2021, Crown Melbourne rated Customer 4's risk as significant.

On 26 August 2021, Crown Melbourne rated Customer 4's risk as high for the first time after a review was conducted.

See paragraph 481.

842. It was not until 28 August 2021 that Customer 4 was rated high risk by Crown Perth.

Particulars

On various occasions between 14 June 2016 and 27 August 2021, Crown Perth rated Customer 4's risk as low.

On 28 August 2021, Crown Perth rated Customer 4's risk as high for the first time. The risk rating was automatically raised as a result of a review conducted by Crown Melbourne.

See paragraph 481.

843. On and from 1 March 2016 designated services provided to Customer 4 posed higher ML/TF risks including because the provision of designated services to Customer 4 involved a combination of the following factors:

a. Customer 4 was a junket operator;

b. Customer 4 was a junket player;

c. Customer 4 received high value financial (table 1, s6) and gaming services (table 3, s6) provided through multiple junket programs: see paragraph 473ff;

d. Customer 4 was a junket operator who facilitated the provision of high value financial and gaming services (tables 1 and 3, s6) to many key players on his junket programs: see paragraph 473ff;

e. between 2010 and 2020, turnover for Customer 4's junket had exceeded $13,657,000,000 at Crown Melbourne and $3,033,000,000 at Crown Perth;

f. designated services provided to Customer 4 lacked transparency as the services were provided through the channel of junket programs: see paragraph 477(e);

g. designated services provided to Customer 4 involved large transfers to and from third parties, including to and from other junket operators, foreign remittance service providers and unknown third parties: see paragraph 456ff:

    i. between 2014 and 2020, Customer 4 transferred funds to 65 unique beneficiaries totalling $53,945,458 and received transfers from 102 unique third-party senders totalling $216,378,493;

    ii. between 2015 and 2020, Customer 4 received deposits totalling $150,338,386 from a network of individuals, company accounts and related entities;

    iii. between 2010 and 2020, Customer 4 received 721 inbound telegraphic transfers totalling $301,950,621 at Crown Melbourne from accounts held in his name and third parties including key players, junket representatives and money remitters;

    iv. between 2010 and 2020, Customer 4 sent 182 outbound telegraphic transfers totalling $90,217,506 at Crown Melbourne;

    v. between 2010 and 2020, Customer 4 received 22 inbound telegraphic transfers totalling $23,229,283 at Crown Perth from accounts held in Customer 4's name and from an Australian casino; and

    vi. between 2015 and 2020, Customer 4 sent 11 outbound telegraphic transfers totalling $13,294,230 at Crown Perth the significant majority of which was sent to Customer 4's Crown Melbourne DAB account.

h. funds transferred to Customer 4 from third parties including key players, junket representatives and money remitters regularly would contain references such as "Investment" and "Investment for property";

i. funds transferred from Customer 4 to other junket operators and representatives included transactions not related to Customer 4's junket;

j. designated services provided to Customer 4 involved large cross-border movements of funds including through the Southbank accounts: see paragraph 239;

k. large values were transferred to and from Customer 4's bank accounts and his DAB account, and to and from other customers' DAB accounts, involving the provision by Crown Melbourne of designated services within the meaning of items 31 and 32, table 1, s6 of the Act: see paragraphs 411ff and 492;

l. by December 2021, Customer 4 made repeated large transactions on his Crown Melbourne safekeeping and DAB accounts:

    i. Customer 4 had made 535 cash deposits totalling $25,747,340 into his safekeeping account. Customer 4 had made 3,883 cash withdrawals totalling $93,561,685 from his safekeeping account;

    ii. Customer 4 had received 90 other transfers totalling $40,696,208 into his safekeeping account. Customer 4 had sent 122 other transfers totalling $53,055,241 from his safekeeping account;

    iii. Customer 4 had used $16,203,303 from his safekeeping account across 12 transactions towards redemptions;

    iv. Customer 4 had deposited 24 bank cheques and one Crown cheque totalling $4,196,800 into his safekeeping account. Customer 4 had withdrawn 34 Crown cheques totalling $9,753,950 from his safekeeping account;

    v. Customer 4 had made 511 threshold cash-ins or deposits totalling $17,028,626 and 409 sub-threshold cash-ins or deposits totalling $1,555,134 from his DAB account. Customer 4 had made 67 threshold cash-outs or withdrawals totalling $3,838,805 and $228,736 in sub-threshold cash-outs or withdrawals from his DAB account;

    vi. Customer 4 had deposited 35 bank cheques and one Crown cheque totalling $6,034,481 into his DAB account. Customer 4 had withdrawn one bank cheque and seven Crown cheques totalling $4,550,000 from his DAB account;

    vii. Customer 4 had received 264 other transfers totalling $143,024,556 into his DAB account and sent 84 other transfers totalling $105,576,329 from his DAB account;

m. by December 2021, Customer 4 made repeated large transactions on his Crown Perth safekeeping and DAB accounts:

    i. Customer 4 had made eight threshold cash-ins or deposits totalling $610,200 and four sub-threshold cash-ins or deposits totalling $19,500 from his DAB account. Customer 4 had made 16 threshold cash-outs or withdrawals totalling $812,550 and $31,825 in sub-threshold cash-outs or withdrawals from his DAB account;

    ii. Customer 4 received 14 other transfers totalling $22,768,958 into his DAB account and four other transfers totalling $4,793,458 from his DAB account;

n. Customer 4 made or received large transfers or unusual requests for transfers to and from other Australian and overseas casinos: see paragraphs 398ff and 407ff;

o. at various times, Customer 4 had significant parked or dormant funds in his DAB accounts: see paragraph 252;

    i. despite the ML/TF risks posed by Customer 4, on 28 June 2021, Crown Melbourne permitted him to transfer the balance of his Crown Melbourne DAB to an international bank account in his name;

p. at various times, Customer 4 was provided with significant amounts of credit upon request, up to limits of $10,000,000: see paragraphs 280ff and 487;

q. Customer 4 or his junket representatives engaged in other transactions indicative of ML/TF typologies, including quick turnover of funds (without betting), cuckoo smurfing, parked funds and structuring: see paragraphs 24 and 252;

r. Crown Melbourne made available the Crown private jet for Customer 4. There were inadequate controls on the carrying of large amounts of cash on Crown's private jets: see paragraphs 454 and 491(c);

s. these transactions took place against the background of:

   i. 79 SMRs given to the AUSTRAC CEO by Crown Melbourne by 1 March 2016;

   ii. by 1 March 2016, Customer 4 had been involved in many large and suspicious third party transactions and transactions indicative of ML/TF typologies involving quick turnover of funds (without betting);

   iii. by 1 March 2016, Customer 4's junket at Crown Melbourne had a turnover of $3,005,469,301 and a loss of $54,280,543;

   iv. by 1 March 2016, Customer 4's junket at Crown Perth had a turnover of $171,672,675 and a loss of $8,004,570;

t. by 2016, Crown Melbourne were aware that Customer 4's junket operated as a sub-junket of a foreign junket tour operator;

u. in 2018, Customer 4 and key players in Customer 4's junket were the subject of law enforcement enquiries on two occasions; and

v. by reason of the matters set out at subparagraphs a. to u. above, there were real risks that Customer 4's source of wealth and source of funds were not legitimate.

Monitoring of Customer 4's transactions

844. At no time did Crown Melbourne or Crown Perth appropriately monitor Customer 4's transactions on a risk-basis.

Particulars

Section 36(1)(a), (b) of the Act and rules 15.4 to 15.8 of the Rules.

Crown Melbourne and Crown Perth were unable to monitor the ML/TF risks posed by Customer 4's transactions appropriately because it did not make and keep appropriate records of designated services provided to junket operators and junket players: see paragraphs 483ff.

Crown Melbourne and Crown Perth were unable to monitor the ML/TF risks posed by transactions associated with Customer 4's junkets, including transactions by his junket representatives and key players on his junkets, because it did not make and keep appropriate records of designated services provided: see paragraphs 483ff.

Crown Melbourne and Crown Perth did not apply appropriate risk-based transaction monitoring to designated services provided to Customer 4: see paragraphs 590ff and 629 to 642 (designated services) and 643 to 649 (transactions facilitated through junkets).

Customer 4's transactions involved repeated transactions indicative of ML/TF typologies that were not detected. Had appropriate risk-based transaction monitoring been applied, these transactions could have been identified earlier: see paragraphs 686 and 687.

Transactions to and from third parties

Between 2010 and 2020, Customer 4 received 721 inbound telegraphic transfers at Crown Melbourne totalling $301,950,621 from accounts held in his name and third parties including key players, junket representatives and money remitters. In the same period, Customer 4 sent 182 outgoing telegraphic transfers at Crown Melbourne totalling $90,217,506: SMR dated 7 December 2021.

Between 2010 and 2020, Customer 4 received 22 inbound telegraphic transfers at Crown Perth totalling $23,299,283 from accounts held in his name and an Australian casino. Between 2015 and 2020, Customer 4 sent 11 outgoing telegraphic transfers at Crown Perth totalling $12,494,230: SMR dated7 December 2021.

According to an independent audit conducted in 2021, between 2 April 2014 and 10 March 2020, Customer 4 transferred funds to 65 unique beneficiaries totalling $53,945,458 over 130 transactions. Only 40 of those were key players in Customer 4's junket. Only 56 transactions, comprising $21,640,640, had known destination countries. One third party alone received $4,078,500.

Between 14 February 2014 and 22 April 2020, Customer 4 received transfers from 102 unique third-party senders totalling $216,378,493 over 511 transactions. Only 37 of those were key players in Customer 4's junket and only 51 had positive matches as Crown Melbourne customers. Only 129 transactions had their source of funds determined, comprising $82,527,888 of the transactions. Where the source of funds was determined, $62,245,148 (75%) of funds originated from two foreign countries.

Between 21 December 2015 and 25 February 2020, Customer 4 received deposits from a network of individuals, company accounts and related entities. Combined, the network transferred $150,338,386 to Customer 4 over 180 transactions. The network included:

- a company account (Company 1) which sent approximately $19,662,972 over 16 transactions between 6 March 2017 and 9 February 2018;
- a second company account (Company 6) which sent $7,360,638 over 13 telegraphic transfers between 21 December 2015 and 18 September 2017;
- a third company account which sent $13,738,400 over 24 telegraphic transfers between 2 February 2016 and 23 December 2016;

- a Crown customer, Customer 4's junket representative, who sent approximately $71,881,319 over 100 telegraphic transfers between 24 June 2017 and 25 February 2020; and
- a money remitter which sent approximately $36,208,990 over 23 transactions between 14 December 2017 and 26 May 2018 and shared the same foreign business address as Company 1's account.

The volume of Customer 4's transactions varied significantly over the period and peaked in 2018. Bank transaction deposits with classification 'NA' totalled $40,320,027 in 2019 and $0 in 2020, whereas 'other' transactions increased from $2,889,963 in 2019 to $16,041,912 in 2020.

Transactions indicative of ML/TF typologies – quick turnover of funds

Transactions involving Customer 4 were identified by an independent auditor in 2021 as indicative of the ML/TF typology of quick turnover of funds (without betting) totalling $18,616,739. On 21 occasions, no gaming activity had occurred:

- on 6 July 2016, two deposits of $68,000 and $43,063 by telegraphic transfer were made into Customer 4's DAB account followed by a withdrawal of $500,000 by telegraphic transfer and $3,000 in cash the following day;
- on 23 May 2017, two deposits of $120,000 by telegraphic transfer and $1,000 in cash were made into Customer 4's DAB account followed by a withdrawal of $161,000 on the following day;
- on 11 June 2017, three deposits of $15,000, $10,000 and $10,000 were made to Customer 4's DAB account followed by two withdrawals of $5,640 and $5,550 in cash on the same day. The following day, a withdrawal of $150,000 by telegraphic transfer and six withdrawals of $28,260, $10,220, $10,000, $7,000, $3,900 and $2,650 in cash were made on Customer 4's DAB account;
- on 2 July 2017, a deposit of $20,000 by telegraphic transfer was made to Customer 4's DAB account followed by two withdrawals of $50,000 and $2,000 in cash on the following day;
- on 16 October 2017, a deposit of $200,000 by telegraphic transfer was made from Customer 4's DAB account followed by a withdrawal of $200,000 by telegraphic transfer and two withdrawals of $60,005 and $15,000 in cash on the same day;
- on 15 January 2018, two deposits of $30,000 and $23,000 by telegraphic transfer were made to Customer 4's DAB account followed by two withdrawals of $60,000 and $1,908 in cash on the following day;

- on 27 March 2018, a deposit of $1,000,000 by telegraphic transfer to Customer 4's DAB account followed by a withdrawal of $1,000,000 by telegraphic transfer on the same day. The following day, five withdrawals of $34,050, $30,000, $10,000, $8,115 and $3,100 in cash were made from Customer 4's DAB account;
- on 9 April 2018, a deposit of $50,000 by telegraphic transfer to Customer 4's DAB account followed by a withdrawal of $100,000 in cash on the same day;
- on 18 April 2018, three deposits of $10,000, $10,000 and $8,000 by telegraphic transfer to Customer 4's DAB account followed by a withdrawal of $50,000 in cash on the same day;
- on 22 April 2018, a deposit of $1,000,000 by telegraphic transfer to Customer 4's DAB account followed by a withdrawal of $1,000,000 by telegraphic transfer on the same day;
- on 21 May 2018, three deposits of $10,000, $6,000 and $5,000 by telegraphic transfer and a deposit of $7,000 in cash to Customer 4's DAB account followed by a withdrawal of $7,490 in cash the following day and three withdrawals of $67,700, $58,700 and $2,000 in cash the day after that;
- on 24 June 2018, a deposit of $20,000 in cash into Customer 4's DAB account followed by a withdrawal of $1,234,130 by telegraphic transfer on the following day;
- on 16 August 2018, four deposits of $20,000, $20,000, $10,000 and $5,000 by telegraphic transfer into Customer 4's DAB account followed by a withdrawal of $50,000 by telegraphic transfer and $22,600, $20,000 and $2,045 in cash on the same day;
- on 17 August 2018, a deposit of $100,000 by telegraphic transfer into Customer 4's DAB account followed by two withdrawals of $101,030 and $12,180 in cash on the same day;
- on 14 October 2018, a deposit of $25,000 by telegraphic transfer into Customer 4's DAB account followed by three withdrawals of $100,000, $30,000 and $1,300 in cash on the same day;
- on 1 November 2018, two deposits of $394,321 and $20,000 by telegraphic transfer and $19,450 in cash into Customer 4's DAB account followed by a withdrawal of $850,888 by telegraphic transfer and two withdrawals of $5,500 and $4,700 in cash on the same day;
- on 8 May 2019, two deposits of $106,227 and $70,000 into Customer 4's DAB account followed by a withdrawal of $1,500,000 by telegraphic transfer and $880 in cash by telegraphic transfer on the same day;

- on 27 May 2019, a deposit of $50,000 by telegraphic transfer into Customer 4's DAB account followed by a withdrawal of $35,000 in cash on the following day and a further withdrawal of $30,000 in cash on the day after that;
- on 21 June 2019, a deposit of $1,031,788 by telegraphic transfer into Customer 4's DAB account followed by a withdrawal of $1,007,500 by telegraphic transfer on the same day. On 22 June 2019, two withdrawals of $210,000 and $10,000 in cash from Customer 4's DAB account followed by a further withdrawal of $3,100 in cash on the following day;
- on 16 December 2019, a deposit of $36,000 in cash into Customer 4's DAB account followed by a withdrawal of $36,000 by telegraphic transfer on the same day; and
- on 4 March 2020, a deposit of $900,000 by telegraphic transfer into Customer 4's DAB account followed by two withdrawals of $800,000 and $65,424 by telegraphic transfer on the same day.

Transactions indicative of ML/TF typologies – junket operator transactions

In 2021, an independent auditor identified Customer 4 as responsive to an ML/TF "risk area" as a result of Customer 4's activity as a junket operator. The independent auditor noted that junkets are high risk for casino ML/TF activity and therefore patrons identified as junket operators, including Customer 4, presented a higher ML/TF risk to Crown Melbourne and Crown Perth.

Transactions indicative of ML/TF typologies – structuring

In March 2019, May 2019, June 2019, September 2019, October 2019, November 2019 and February 2020, Customer 4 engaged in transactions identified by an independent auditor in 2021 as indicative of the ML/TF typology of structuring of deposits, totalling $116,100.

Transactions indicative of ML/TF typologies – cuckoo smurfing

Customer 4 engaged in transactions identified by an independent auditor in 2020 as indicative of the ML/TF typology of cuckoo smurfing.

On 30 March 2016, Customer 4 received two transfers from international third party companies indicative of the ML/TF typology of cuckoo smurfing.

Between 31 August 2017 and 29 June 2018, Customer 4 was involved in five transfers from international third party individuals indicative of the ML/TF typology of cuckoo smurfing.

Between 13 December 2017 and 12 November 2019, Customer 4 was involved in 95 transfers by overseas money remitters indicative of the ML/TF typology of cuckoo smurfing.

Transactions indicative of ML/TF typologies – third party transfers

Customer 4 engaged in transactions identified by an independent auditor in 2021 as indicative of the ML/TF typology of third party transfers through a Crown patron account at Crown Melbourne and Crown Perth and the Southbank accounts.

Transactions indicative of ML/TF typologies – parked funds

Customer 4 engaged in transactions identified by an independent auditor in 2021 as indicative of the ML/TF typology of parked funds. Between 24 November 2020 and at least 18 June 2021, Customer 4's DAB account had a balance of $7,079,089. Customer 4 had the highest balance of parked funds of any Crown Melbourne customer.

On 28 June 2021, Customer 4 transferred the balance of his Crown Melbourne DAB to an international bank account in his name: SMR dated 7 December 2021.

Inadequate controls on Crown's private jets

On 11 August 2016, Crown Melbourne provided Customer 4 with access to a Crown private jet to facilitate travel from Melbourne to Sydney for two people.

There were inadequate controls on the carrying of large amounts of cash on Crown's private jets*:* see paragraphs 454 and 491(c).

Ongoing customer due diligence

845. On and from 1 March 2016, on multiple occasions, the provision of designated services to Customer 4 raised red flags reflective of higher ML/TF risks as a result of Customer 4's frequent, large transactions with a number of third parties included repeated transactions with a network of third party companies.

Particulars

See paragraph 456ff.

Large and suspicious third party transactions in 2016

In 2016, Customer 4 received by telegraphic transfer approximately $6,649,344 from third parties, including:

- on 23 March 2016 and 4 July 2016, $1,009,614 and $506,465 from a company account;
- on 4 July 2016, $699,123 from Crown Perth;
- on 24 August 2016 and 25 August 2016, $416,150 and $1,000,000 from an Australian casino;
- on 1 September 2016, $1,000,000 from an Australian casino; and
- on 16 September 2016, $994,644 from Company 6's account.

In 2016, Customer 4 sent by telegraphic transfer approximately $2,509,591 to third parties, including:

- on 25 August 2016, $1,500,000 to a third party.

Large and suspicious third party transfers in 2017

In 2017, Customer 4 received by telegraphic transfer approximately $5,064,888 from third parties and sent by telegraphic transfer approximately $1,450,000 to third parties, including:

- on 4 January 2017 and 31 October 2017, $500,000 and $1,000,000 from an Australian casino;
- on 29 March 2017, $100,000 from an Australian casino;
- on 30 June 2017, $1,100,000 from a company in an Australian casino group; and
- on 30 October 2017, $2,085,821 from a company account (Company 1).

Large and suspicious third party transfers in 2018

In 2018, Customer 4 received by telegraphic transfer approximately $8,282,815 from third parties, including:

- on 2 January 2018 and 9 February 2018, $289,465 and $1,945,781 from a company account (Company 1);
- on 13 April 2018, $3,664,540 from Crown Perth;
- on 1 August 2018, $959,911 from a company account;
- on 14 August 2018, $974,658 from a Crown customer and Customer 4's junket representative, Person 7;
- on 26 September 2018 and 27 September 2018, a total of $1,000,000 from a third party;
- on 29 October 2018, $1,000,000 from an Australian casino;
- on 27 October 2018 and 30 October 2018, a total of $1,000,000 from a Crown customer and Customer 4's junket representative, Person 7;
- on 31 December 2018, $1,002,606 from a Crown customer and Customer 4's junket representative, Person 7;

In 2018, Customer 4 sent by telegraphic transfer approximately $1,420,000 to third parties, including:

- on 2 August 2018, $1,000,000 to a third party.

Large and suspicious third party transactions in 2019

In 2019, Customer 4 received by telegraphic transfer approximately $8,324,039 from third parties and sent by telegraphic transfer approximately $2,001,400 to third parties, including:

- on 6 March 2019, $1,021,033 from a Crown customer and Customer 4's junket representative, Person 7;

- on 30 July 2019, 31 July 2019 and 1 August 2019, $2,000,000 from a Crown customer and Customer 4's junket representative, Person 7;
- on 5 September 2019, $1,000,000 from a Crown customer and Customer 4's junket representative, Person 7; and
- on 30 October 2019, $1,100,000 from a Crown customer and Customer 4's junket representative, Person 7.

846. On and from 1 March 2016, on multiple occasions, the provision of designated services to Customer 4 raised red flags reflective of higher ML/TF risks as a result of complex, unusual large transactions and unusual patterns of transactions involving Customer 4 which had no apparent economic or visible lawful purpose.

Particulars

Unusual transactions and patterns of transactions in 2016

On 27 June 2016, a Crown Perth customer transferred $123,300 from their DAB account to Customer 4's Crown Melbourne DAB account. Crown Perth were unaware of any relationship between the customers: SMR dated 27 June 2016.

On 14 July 2016, a Crown Perth customer transferred $699,123 from their DAB account to Customer 4's Crown Melbourne DAB account. Crown Perth were unaware of any relationship between the customers: SMR dated 14 July 2016.

Unusual transactions and patterns of transactions in 2017

On 8 February 2017, Crown Melbourne received an email from an Australian financial services license holder (Company 4) which stated that it conducted transfers to Crown Melbourne via another company, Company 1. On and from 30 October 2017, this company made many large deposits into Customer 4's Crown Melbourne DAB totalling approximately $19,662,972.

On 5 December 2017, Customer 4 transferred $721,600 from his DAB account to another junket operator: SMR dated 6 December 2017. The transfer was made for the purpose of allowing the other junket operator to provide front money to a key player in the junket program.

Unusual transactions and patterns of transactions in 2018

On 9 February 2018, $1,945,870.50 was received by Crown Melbourne from Company 1's account to be applied to Customer 4's DAB account. However, despite the 8 February 2017 email received by Crown Melbourne, no link had been established between the Australian financial services license holder (Company 4) and the company making the transfer (Company 1).

Unusual transactions and patterns of transactions in 2019

In FY2019, $50,093,448 was transferred into Customer 4's Crown Melbourne DAB account from his personal account, third parties, key

players and company accounts. $34,278,706 of that amount (68%) was transferred by a single individual being Customer 4's junket representative, Person 7. $15,550,620.60 was transferred out of Customer 4's Crown Melbourne DAB account to Crown Perth, third parties, key players or company accounts.

Unusual transactions and patterns of transactions in 2020

On 7 January 2020, a Crown Perth customer and Customer 4's junket representative, Person 7, transferred $1,000,000 from his account at another Australian casino to Customer 4's Crown Perth DAB account for redemption. Customer 4 did not owe money to Crown, but Crown Perth were unable to verify whether the Crown Perth customer owed money to Customer 4 in respect of junket activity. Crown Perth senior management were aware that Customer 4 was operating a junket at the other Australian casino under the Crown Perth customer's name.

In February 2020, the Group General Manager (Anti-Money Laundering) and a Manager (Program Compliance) determined that there were no reasonable grounds for suspicion in respect of this transaction as it was known that a high value patron's assistant, or an employee of a foreign-based junket operator, would register as the junket operator.

On 28 February 2020, two telegraphic transfers were received for Customer 4's junket totalling $50,000 from Person 27, a junket representative of another junket operator (Customer 14). The funds were transferred for a key player of Customer 4's junket who was a friend of the junket representative.

In March 2020, Customer 4 operated a junket at Crown Perth with only one key player. On 4 March 2020, the key player transferred $900,000 to Customer 4 as front money. The junket settled on the same day and Customer 4 transferred $800,000 back to the key player. The junket program recorded a loss of $200,000, given $20,845 in 'ecom' and paid $145,912 in commission. Crown Perth reported that that this series of transactions was made because the key player had depleted $1,500,000 in junket funds, had lost $200,000 but given the key player in commission and so sent the key player back $800,000.

847. On and from 1 March 2016, on multiple occasions, the provision of designated services to Customer 4 raised red flags reflective of higher ML/TF risks as a result of Customer 4's junket activity.

Particulars

See paragraph 477.

From at least 3 October 2016, Customer 4's junket was approved for a 60% rebate on win/loss programs at Crown Perth and Crown Melbourne.

In January 2017, Customer 4 requested that the name of his junket be changed to that of a relative, Person 18, who had previously been detained in China. This request was the subject of several VIP Operations meetings pleaded at paragraph 848.

By 2016, Crown Melbourne were aware that Customer 4's junket was a sub-junket of a foreign junket operator.

Between 1 August 2018 and 31 August 2018, Customer 4 ran a junket program and played as a key player in his junket.

Between 2016 and 2020, Customer 4's junket at Crown Melbourne had a turnover of $10,651,826,082 and a loss of $193,989,123:

- in 2016, Customer 4's junket had a turnover of $2,289,374,560 and a loss of $59,584,123;
- in 2017, Customer 4's junket had a turnover of $1,674,840,400 and a loss of $34,699,517;
- in 2018, Customer 4's junket had a turnover of $4,167,900,329 and a loss of $46,044,020;
- in 2019, Customer 4's junket had a turnover of $2,331,243,533 and a loss of $52,459,549; and
- in 2020, Customer 4's junket had a turnover of $188,467,260 and a loss of $1,201,914.

Between 2016 and 2020, Customer 4's junket at Crown Perth had a turnover of $2,861,416,826 and a loss of $5,548,361:

- in 2016, Customer 4's junket had a turnover of $6,532,075 and a loss of $519,830;
- in 2017, Customer 4's junket had a turnover of $2,564,255 and a loss of $31,809;
- in 2018, Customer 4's junket had a turnover of $1,641,003,721 and a loss of $19,642,342;
- in 2019, Customer 4's junket had a turnover of $1,062,724,475 and a win of $18,291,410; and
- in 2020, Customer 4's junket had a turnover of $148,592,300 and a loss of $3,645,790.

848. On and from 1 March 2016, on multiple occasions, the provision of designated services to Customer 4 raised red flags reflective of higher ML/TF risks as a result of receiving numerous enquiries from law enforcement agencies in respect of Customer 4 and key players in his junket.

Particulars

On 29 May 2018, key players in Customer 4's junket were the subject of a law enforcement enquiry. The requests were for video footage of suspicious deposits made by those key players in December 2017 totalling $1,225,000.

On 5 July 2018, Crown Melbourne received a law enforcement enquiry in respect of Customer 4.

849. At no time did Crown Melbourne or Crown Perth undertake appropriate risk-based customer due diligence with respect to Customer 4 with a view to identifying, mitigating and managing the ML/TF risks posed by the provision of designated services on and from 1 March 2016.

Particulars

Section 36(1)(a) of the Act.

a. At no time did Crown Melbourne or Crown Perth take appropriate steps to understand Customer 4's source of wealth/funds was legitimate.

b. At no time did Crown Melbourne or Crown Perth take appropriate steps to identify or analyse the ML/TF risks of Customer 4's transactions or to consider whether they had a lawful purpose.

c. With the exception of two transactions in April 2016, one transaction in February 2018, one transaction in January 2020 and one transaction in February 2020, Crown Melbourne and Crown Perth gave no consideration at any time to whether large and high risk transactions should be processed. Other than the April 2016 transactions, each transaction was ultimately allowed by Crown Melbourne or Crown Perth despite the ordering company having no demonstrable connection with Customer 4 or his junket operations.

d. On a number of occasions, Crown Melbourne considered the basis for large and high risk transactions involving Customer 4. In two cases, Crown Melbourne senior management considered large and high risk transactions for the purpose of determining whether or not to give the AUSTRAC CEO an SMR. In each case, the transaction had been processed before it was considered. On all occasions other than in respect of two transactions in April 2016, the transactions were processed and not rescinded.

e. On each occasion that senior management considered whether to continue the business relationship with Customer 4, senior management failed to give adequate consideration to whether the ML/TF risks posed by Customer 4 were within Crown Melbourne and Crown Perth's risk appetite.

Particulars

Due diligence

In December 2021, as part of Crown Melbourne and Crown Perth's lookback program, each entity gave the AUSTRAC CEO an SMR. The SMRs identified that:

- in 2016, Crown had obtained a wealth report which identified Customer 4 to be the director and shareholder of a business which owned an Australian restaurant. Crown had identified Customer 4 as the operator of a sub-junket of an international junket business. Crown had identified Customer 4 to be the primary operator of the international junket business with close personal ties to the owner and founder of the international junket business;

- in 2019, further due diligence searches were attempted. These searches did not allow Crown to construct a credible valuation of Customer 4's business interests or wealth. Further background checks were attempted but did not yield any positive results beyond potential matches. Crown held a business card for Customer 4 which identified him to be the chairman and president of a property development company. Risk intelligence, open media report and other open-source searches returned no adverse results in respect of Customer 4; and
- while a customer at Crown Melbourne and Crown Perth, no due diligence conducted provided a basis for Crown to understand Customer 4's source of wealth/funds with respect to the designated services it was providing to him and to determine its legitimacy.

In December 2021, Crown Melbourne and Crown Perth recognised that no due diligence conducted provided a basis for Crown to understand Customer 4's source of wealth/funds with respect to the designated services it was providing to him and to determine its legitimacy.

Request to transfer country registration of junket in 2016

In November 2016, an individual in Customer 4's junket asked Crown Melbourne senior management that Customer 4's junket be registered in a different foreign country. Customer 4's foreign passport, ID, utility bills and two bank account passbooks were provided for that purpose.

In December 2016, a VIP Operations meeting took place in which Crown Melbourne senior management requested that due diligence be conducted in respect of Customer 4. A further VIP Operations meeting identified that Customer 4 had originally been registered as a junket in a particular foreign country because of his primary place of address, but had since provided documentation to register the junket in another foreign country. A junket due diligence profile was noted to have been prepared for Customer 4.

Request to transfer name of junket in 2017

In January 2017, two VIP Operations meeting took place. The meeting notes identified that Crown was unable to confirm an official link between Customer 4 and the foreign junket operator and that Customer 4 had requested that the junket be transferred into the name of his relative, Person 18. Crown staff were instructed to speak to Customer 4 and ask him to apply to be an approved collaborator with a foreign junket regulator and to determine why Customer 4 wanted to move junket operations into the name of his relative Person 18, why that relative was detained in a foreign country, how he obtained bail and whether he could travel to Australia.

Consideration of large and unusual transactions

On several occasions, Crown gave consideration to whether large and high risk transactions should be investigated. However, other than in April 2016, the transactions were processed despite the higher ML/TF risk they posed.

In April 2016, a Credit control coordinator sent two emails to an Australian bank requesting the urgent return of funds and attaching authority in support. The relevant transactions were amounts deposited into Crown Melbourne's account for Customer 4 from two company accounts of $499,990 and $499,970.

In February 2018, in response to a telegraphic transfer of $1,945,780 being received for Customer 4 from Company 1's account the Senior Vice President (International Business) emailed the Chief Legal Officer identifying that Customer 4 was a longstanding junket operator who ordinarily used an Australian financial services licence holder (Company 4) to conduct transfers into Crown Melbourne. The Senior Vice President (International Business) said that the licence holder uses another company, Company 1, to conduct the transfers. However, Crown Melbourne were unable to establish an ownership link between the licence holder and the other company other than an email sent to Crown Melbourne in February 2017 from the licence holder. On the basis of that email alone, funds had been accepted previously. The email attached company searches conducted in February 2018 for the two purportedly related entities, which did not identify a link between them.

In January 2020, after Customer 4 received a telegraphic transfer into his Crown Perth DAB of $1,000,000 from an Australian casino account held in the name of another Crown Perth customer (Customer 4's junket representative), Crown Perth senior management investigated the purpose of this transaction. Crown Perth were aware that Customer 4 was operating a junket at an Australian casino under the other customer's name. The AML Compliance Manager indicated that the purpose of the transfer could be because, first, the money was coming from the other customer's personal account or, second, the other Australian casino junket was in that other customer's name.

In February 2020, after Customer 4 received two telegraphic transfers totalling $50,000 from Person 27, a junket representative for another junket operator (Customer 14), the CTRM emailed Crown Melbourne Cage management and copied into the AML Melbourne team and the VIP Banking team. The CTRM asked about the relationship between Customer 4 and the junket representative. A Director (International Business Operations) responded stating that the junket representative was a friend of a key player in Customer 4's junket and the funds were for the key player.

Other than in April 2016, Crown did not take appropriate steps in considering whether large and high risk transactions should be processed.

Other due diligence conducted

Between March 2016 and January 2020, Crown conducted Australian and foreign company searches in respect of Customer 4 and obtained company reports in respect of companies associated with Customer 4.

Between March 2016 and February 2020, Crown conducted land registry searches in respect of Customer 4.

Between August 2016 and August 2020, Crown conducted risk intelligence searches in respect of Customer 4 which returned multiple results, some of which were designated "political individual" and others of which were designated "crime – financial".

Between December 2016 and March 2019, Crown conducted open source searches in respect of a foreign junket organisation thought to be linked to Customer 4.

In November 2019, Crown prepared a junket profile in respect of Customer 4 with the recommendation that Crown continue to conduct business with Customer 4. The profile summarised information known about Customer 4 but there was no evidence that his ML/TF risk was considered in respect of the recommendation.

On 28 July 2020, a Credit Supervisor requested a surveillance check for Customer 4. Crown Melbourne and Crown Perth surveillance analysts replied that there were no gaming integrity concerns with Customer 4 as a junket operator in the SEER database.

None of these steps were proportionate to the ML/TF risks reasonably posed by Customer 4 on and from 1 March 2016.

Enhanced customer due diligence

850. Having formed a suspicion for the purposes of s41 of the Act, between 24 March 2016 and 7 January 2022, Crown Melbourne gave the AUSTRAC CEO 96 SMRs in respect of Customer 4: Schedule 3.4.2.

Particulars

Each of these SMRs reported high losses and 'minimal individual rated gaming activity' noting that 'win/losses under a junket program are not shown under a patron's individual rated gaming activity'.

Collectively, the SMRs given to the AUSTRAC CEO between 24 March 2016 and 4 August 2021 reported transfers from Customer 4's DAB account to third parties, key players or company accounts totalling $15,623,348 and transfers to Customer 4's DAB account from third parties, key players or company accounts totalling $9,597,341.

The telegraphic transfers included large cross-border movement of funds to individuals and companies unknown to Crown Melbourne.

The majority of SMRs related to losses recorded for junket key players which was often not in line with historic gaming activity for the junket player involved. Some SMRs related to payments to third parties, both individuals and entities, who were not listed as a key player in a junket.

In respect of four SMRs, junket key players made a loss under the junket program but were transferred funds from the junket rather than paying the junket: SMRs dated 2 January 2019, 1 April 2019, 9 May 2019 and 1 November 2019.

In respect of three SMRs, junket key players received funds significantly in excess of the amount that they won under the junket program: SMRs dated 1 August 2019, 6 September 2019 and 14 November 2019.

Other suspicious activity reported by the SMRs included:

- a key player in Customer 4's junket withdrawing $100,000 for use in gaming machines but the majority of the funds being immediately returned by a junket representative: SMR dated 5 October 2017;
- a junket representative withdrawing $800,000 in cash from Suncity in $50,000 bundles comprising $50 notes to be deposited to the junket in circumstances where all Suncity staff refused to sign any document in connection with this transaction: SMR dated 16 October 2017;
- a foreign junket key player making a payment of $100,000 to the junket with the reference "Purchase Investment Property", which was returned by Crown as not being for gaming purposes: SMR dated 15 March 2018;

The December 2021 SMR comprised the Crown Melbourne and Crown Perth lookback contained in paragraph 844.

851. Having formed a suspicion for the purposes of s41 of the Act, Crown Perth gave the AUSTRAC CEO SMRs with respect to Customer 4 on:

a. 27 June 2016;

b. 14 July 2016; and

c. 8 May 2019;

d. 7 December 2021; and

e. 14 December 2021 (x 2).

Particulars

Each of these SMRs reported described, among other things, the wins and losses of key players in Customer 4's junket, telegraphic transfers sent or received for Customer 4 from key players without

rated play to justify them, third party transactions (domestic and international) who were not key players, transactions with other casinos and other suspicious behaviour of players in Customer 4's junket.

The December 2021 SMR comprised the Crown Melbourne and Crown Perth lookback contained in paragraph 844.

852. On each occasion that Crown Melbourne and Crown Perth formed a suspicion with respect to Customer 4 for the purposes of s41 of the Act, it was required to apply its ECDD program to Customer 4.

Particulars

Rule 15.9(3) of the Rules.

853. Crown Melbourne and Crown Perth did not carry out appropriate risk-based ECDD measures with respect to Customer 4 on each occasion that Crown Melbourne or Crown Perth formed a suspicion with respect to Customer 4 for the purposes of s41 of the Act.

a. There are no records of any ECDD being conducted after giving the AUSTRAC CEO any SMRs: see paragraphs 664 and 685.

b. Appropriate risk-based steps were not taken to obtain or analyse information about Customer 4's source of wealth/funds: see paragraph 667.

c. Appropriate risk-based steps were not taken to analyse and monitor Customer 4's transactions – both past and future – including to understand their economic purpose: see paragraphs 590 and 666.

d. On each occasion that senior management considered whether to continue the business relationship with Customer 4, senior management failed to give adequate consideration to whether the ML/TF risks posed by Customer 4 were within Crown Melbourne and Crown Perth's risk appetite: see paragraph 668ff.

Particulars

Rule 15.9(3), rule 15.10(1)(c), (d), (2), (5) and (6) of the Rules.

While some due diligence was conducted contemporaneously with the filing of a small number of SMRs, these searches returned no relevant information in respect of Customer 4 and in particular his source of wealth/funds. The steps taken did not constitute ECDD.

See particulars to paragraph 849.

854. By reason of the matters pleaded from paragraphs 832 to 853, on and from 1 March 2016, Crown Melbourne and Crown Perth:

a. did not monitor Customer 4 in relation to the provision of designated services, with a view to identifying, mitigating and managing the ML/TF risks reasonably faced; and

b. did not do so in accordance with rr15.5 and 15.9 of the Rules.

855. By reason of the matters pleaded at paragraph 854, Crown Melbourne and Crown Perth contravened s36(1) of the Act on and from 1 March 2016 with respect to Customer 4.

Particulars

Section 36(1) of the Act is a civil penalty provision: s36(2) of the Act.

Customer 5

856. Customer 5 was a customer of Crown Melbourne from 23 February 2007 to 22 June 2021.

857. From at least 23 February 2007, Crown Melbourne provided Customer 5 with designated services within the meaning of table 1 and table 3, s6 of the Act.

858. From at least 24 April 2014 to 17 March 2020, Customer 5 received designated services as a junket operator at Crown Melbourne.

Particulars to paragraphs 857 and 858

On 23 February 2007, Crown Melbourne opened a DAB account and safekeeping account (AUD/HKD) under a PID for Customer 5. On 11 November 2021, Crown Melbourne closed the accounts.

On 24 April 2014, Crown Melbourne entered into a NONEGPRA with Customer 5 to operate junkets at Crown Melbourne.

Between 2014 and 2020, Customer 5 facilitated at least 155 junkets at Crown Melbourne and Crown Perth for a total of 488 key players.

Between 4 March 2016 and 17 March 2020, Customer 5 operated 65 junket programs under one PID and one program under a second PID at Crown Melbourne. In that period, Customer 5 had approximately 43 junket representatives, including Customer 43.

On 9 May 2014, Crown Melbourne approved a credit facility (AUD/HKD) for Customer 5 under the first PID.

On 23 November 2020, Crown Melbourne closed Customer 5's credit facility under the first PID.

On 22 June 2021, Crown Melbourne issued an indefinite WOL with respect to Customer 5.

859. Customer 5 was a customer of Crown Perth from 3 October 2006 to 22 June 2021.

860. From at least December 2006, Crown Perth provided Customer 5 with designated services within the meaning of table 1 and table 3, s6 of the Act.

861. From at least June 2014 to 27 May 2021, Customer 5 received designated services as a junket operator at Crown Perth.

Particulars to paragraphs 860 and 861

On 3 October 2006, Crown Perth opened a DAB account and safekeeping account (AUD) for Customer 5 under a PID.

On 24 April 2014, Crown Melbourne entered into a NONEGPRA with Customer 5 to operate junkets at Crown Melbourne.

Between 2014 and 2020, Customer 5 facilitated at least 155 junkets at Crown Melbourne and Crown Perth for a total of 488 key players.

Between 24 March 2016 and 22 March 2020, Customer 5 operated 64 junket programs under one PID and 3 junket programs under a second PID. In that period, Customer 5 had approximately 21 unique junket representatives.

On 12 June 2014, Crown Perth opened a second DAB account and safekeeping account (AUD/HKD) for Customer 5 under a second PID.

On 12 June 2014, Crown Perth approved a FAF for Customer 5 connected to 4 different PIDs.

On 30 July 2014, Crown Perth opened a third DAB account and safekeeping account for Customer 5 under a third PID.

On 3 June 2020, Customer 5's HKD DAB account balance of HKD2,655,000 (approx. $508,620) was transferred to his AUD DAB account.

On 27 May 2021, Customer 5's DAB account balance of $679,110 was transferred to his foreign bank account.

On 22 June 2021, Crown Perth issued an NRL with respect to Customer 5.

The ML/TF risks posed by Customer 5

862. By 1 March 2016, higher ML/TF risks were indicated by the nature and purpose of Customer 5's business relationship with Crown Melbourne, the nature of the transactions he had been conducting, together with the suspicions Crown Melbourne itself had formed with respect to Customer 5.

Particulars

Section 36(1)(a), (b) of the Act and Chapter 15 of the Rules.

Junket activity

Customer 5 was a junket operator. He received designated services through the channel of junket programs. This channel lacked transparency: see paragraph 477.

Customer 5 was the son of a junket operator who had operated junkets at Crown Melbourne for over 20 years. From around May 2014, Customer 5 took over the junket operations at Crown Melbourne from his mother following her retirement.

Crown Melbourne recorded that gaming activity on junket programs run by Customer 5 at Crown Melbourne in 2014 involved buy-in of $18,499,200, losses of $3,290,590, and turnover of $121,082,200.

Crown Melbourne recorded that gaming activity on junket programs run by Customer 5 at Crown Melbourne in 2015 involved buy-in of $28,309,300, losses of $4,440,420, and turnover of $446,497,150.

SMRs

By 1 March 2016, Crown Melbourne had given the AUSTRAC CEO 15 SMRs in relation to Customer 5.

Eleven SMRs related to patterns of suspicions relating to key player wins and losses under Customer 5's junket programs – on 4 July 2014, 19 August 2014, 13 November 2014, 18 November 2014, 12 January 2015, 10 August 2015, 24 August 2015, 6 October 2015, 2 December 2015, 5 January 2016 and 26 February 2016. Collectively, the SMRs given to the AUSTRAC CEO between 4 July 2014 and 26 February 2016 reported total wins of $1,707,640 and total losses of $12,189,805.

Three SMRs related to transactions with unrelated third parties, on 6 August 2015, 23 December 2015, and 27 January 2016.

The remaining SMR dated 30 September 2015 related to unusual activity by a junket representative of Customer 5's junket, which reported that Customer 5's junket representative had presented a sports bag on 29 September 2015 containing $400,000 in unmarked $50 notes wrapped in rubber bands for deposit into Customer 5's Crown DAB account.

Due diligence

By 1 March 2016, the only recorded due diligence steps taken with respect to Customer 5 was a risk intelligence search on 15 February 2016.

863. By 1 March 2016, higher ML/TF risks were indicated by the nature and purpose of Customer 6's business relationship with Crown Perth, the nature of the transactions he had been conducting, together with the suspicions Crown Perth itself had formed with respect to Customer 5.

Particulars

Section 36(1)(a), (b) of the Act and Chapter 15 of the Rules.

Junket activity

Customer 5 was a junket operator. He received designated services through the channel of junket programs. This channel lacked transparency: see paragraph 477.

Customer 5 was the son of a junket operator who had operated junkets at Crown Perth for over 20 years. From around June 2014, Customer 5 took over the junket operations at Crown Perth from his mother following her retirement.

Crown Perth recorded that gaming activity on junket programs run by Customer 5 at Crown Perth in 2014 involved buy-in of $29,581,020, losses of $10,290,360, and turnover of $479,886,400.

Crown Perth recorded that gaming activity on junket programs run by Customer 5 at Crown Perth in 2015 involved buy-in of $12,406,775, losses of $2,993,275, and turnover of $53,274,483.

SMRs

By 1 March 2016, Crown Perth had given the AUSTRAC CEO three SMRs in relation to Customer 5. Two SMRs related to telegraphic transfers with unrelated third parties on 4 November 2015 and 23 December 2015.

The remaining SMR dated 24 February 2016 described the deposit of funds and withdrawal of a chip purchase voucher for $150,000 by Customer 5 with no subsequent recorded play.

Between 2014 and 2016, Customer 5 engaged in transactions indicative of ML/TF typologies involving quick turnover of funds (without betting) at Crown Perth:

- on 6 August 2014, Customer 5 deposited $80,000 using cash, then withdrew $254,960 and $576,790 from his DAB account by telegraphic transfer on the same day;
- on 23 July 2015, Customer 5 deposited $100,000 by telegraphic transfer, then withdrew $100,000 in cash from his DAB account on the same day;
- on 6 August 2015, Customer 5 deposited $435,000 in cash, then withdrew $500,000 from his DAB account by telegraphic transfer on the same day; and
- on 3 February 2016, Customer 5 deposited $50,000, $50,000 and $50,000 by telegraphic transfer, then withdrew $150,000 from his DAB account by telegraphic transfer on the same day.

By 1 March 2016, the due diligence steps taken with respect to Customer 5 included a risk intelligence search on 15 February 2016.

864. As at 1 March 2016, Customer 5 should have been recognised by Crown Melbourne as a high risk customer for the reasons pleaded at paragraph 862.

Particulars

Section 36(1)(a), (b) of the Act and Chapter 15 of the Rules.

865. At all times on and from 1 March 2016, Customer 5 should have been recognised by Crown Melbourne as a high risk customer by reason of the matters pleaded at paragraphs 862, 870, 871, 872, 873, 874, and 877.

Particulars

Section 36(1)(a), (b) of the Act and Chapter 15 of the Rules.

866. It was not until 3 June 2021 that Customer 5 was rated high risk by Crown Melbourne.

Particulars

On various occasions between 4 July 2014 and 9 November 2017, Crown Melbourne assessed Customer 5 as moderate risk.

On 9 occasions between 19 November 2017 and 14 January 2019, Crown Melbourne assessed Customer 5 as significant risk.

On 13 June 2019 and 28 October 2019, Crown Melbourne assessed Customer 5 as moderate risk.

See paragraph 481.

867. As at 1 March 2016, Customer 5 should have been recognised by Crown Perth as a high risk customer for the reasons pleaded at paragraph 863.

Particulars

Section 36(1)(a), (b) of the Act and Chapter 15 of the Rules.

868. At all times on and from 1 March 2016, Customer 5 should have been recognised by Crown Perth as a high risk customer by reason of the matters pleaded at paragraphs 863, 870, 871, 872, 873, 874, 875 and 880.

Particulars

Section 36(1)(a), (b) of the Act and Chapter 15 of the Rules.

869. It was not until 1 July 2021 that Customer 5 was rated high risk by Crown Perth.

Particulars

On 17 October 2014 and 4 November 2015, Crown Perth assessed Customer 5 as low risk.

On various occasions between 27 November 2015 and 24 December 2019, Crown Perth assessed Customer 5 as moderate risk.

See paragraph 481.

870. On and from 1 March 2016, designated services provided to Customer 5 by Crown Melbourne and Crown Perth posed higher ML/TF risks including because the provision of designated services to Customer 5 involved a combination of the following factors:

a. Customer 5 received high value financial services (table 1, s6) and gaming services (table 3, s6), through multiple junket programs: see paragraph 473ff;

b. Customer 5 was a junket operator who facilitated the provision of high value financial and gaming services (tables 1 and 3, s6) to least 488 key players (including foreign PEPs) on his junket programs: see paragraph 473ff;

c. by no later than early 2020, Crown Melbourne recorded that turnover on Customer 5's junket had exceeded $2,123,510,915 at Crown Melbourne;

d. by no later than early 2020, Crown Perth recorded that turnover on Customer 5's junket had exceeded $1,139,596,516 at Crown Perth;

e. Customer 5 had taken over the junket operations business of his mother, a junket operator who had operated at Crown Melbourne and Crown Perth for over 20 years, whose turnover prior to 2014 had exceeded $6,650,000,000, and who was of interest to law enforcement in connection with money laundering;

f. Customer 5 was known at all times to be connected to other junket operators, including junket operators in respect of whom Crown Melbourne or Crown Perth had formed suspicions;

g. designated services provided to Customer 5 lacked transparency as the services were provided through the channel of junket programs: see paragraph 477(e);

h. Customer 5, and persons associated with his junket, transacted using large amounts of cash and cash that appeared suspicious, including large volumes of cash in small notes in rubber bands/plastic bags and counterfeit cash: see paragraphs 450, 451, 452 and 491;

i. the table 3, s6, designated services provided to Customer 5 involved high turnover;

j. designated services provided to Customer 5 involved large transfers to and from third parties, including to and from other junket operators, foreign remittance service providers and unknown third parties: see paragraph 456ff;

k. funds transferred from Customer 5 to other junket operators and representatives included transactions related to debt settlement or offsets not related to Customer 5's junket;

l. designated services provided to Customer 5 involved large cross-border movements of funds, including through the Southbank and Riverbank accounts: see paragraph 239;

m. large values were transferred to and from Customer 5's bank accounts and his DAB account, and to and from other customers' DAB accounts, involving designated services within the meaning of items 31 and 32, table 1, s6 of the Act: see paragraphs 411ff and 492;

n. at various times, Customer 5 was provided with significant amounts of credit, including a standing credit line with a limit of $5,000,000, which was reapproved on a regular basis from 2017: see paragraphs 280ff and 487;

o. Customer 5 engaged in suspicious transactions on the Crown Perth HKD currency account, in circumstances where it was not possible to establish a link between the HKD transactions and any junket program run by Customer 5: see paragraph 447;

p. Customer 5 made large transfers or unusual requests for transfers to and from other Australian and overseas casinos: see paragraphs 398ff and 407ff;

q. at various times, Customer 5 had significant parked or dormant funds in his DAB accounts: see paragraph 252;

r. Customer 5 or his junket representatives engaged in other transactions indicative of ML/TF typologies, including structuring, offsetting (including with unrelated third parties), cashing-in large value chips with no evidence of play, and quick turnover of funds (without betting);

s. these transactions took place against the background of 15 SMRs being given to the AUSTRAC CEO by Crown Melbourne and 3 SMRs being given by Crown Perth by 1 March 2016;

t. in 2017, Customer 5 was the subject of law enforcement enquiries on two occasions, and Crown Melbourne reported Customer 5's junket representatives to a law enforcement agency on one occasion; and

u. by reason of the matters set out at subparagraphs a. to t. above, there were real risks that Customer 5's source of wealth and source of funds were not legitimate.

Monitoring of Customer 5's transactions

871. At no time did Crown Melbourne or Crown Perth appropriately monitor Customer 5's transactions on a risk-basis.

Particulars

Section 36(1)(a), (b) of the Act and rules 15.4 to 15.8 of the Rules..

Crown Melbourne and Crown Perth were unable to monitor the ML/TF risks posed by Customer 5's transactions appropriately because they did not make and keep appropriate records of designated services provided to junket operators: see paragraphs 483ff.

Crown Melbourne and Crown Perth did not apply appropriate risk-based transaction monitoring to designated services provided to Customer 5: see paragraphs 590ff and 629 to 642 (designated services) and 643 to 649 (transactions facilitated through junkets).

Lookback

Customer 5's transactions involved repeated transactions indicative of ML/TF typologies (see paragraph 24) that were not detected prior to a 2021 lookback. Had appropriate risk-based transaction monitoring been applied, these transactions could have been identified earlier: see paragraphs 686 and 687.

Customer 5 engaged in the following transactions at Crown Melbourne between 2014 and 2020 (SMR dated 1 July 2021):

- 37 sub-threshold cash deposits totalling $73,869;
- 15 sub-threshold cash withdrawals totalling $50,740;
- 53 threshold cash-ins (across his deposit account, direct cashier or table exchanges) totalling $7,740,062;
- eight threshold cash-outs totalling $516,985 (either from his deposit account or direct cashier exchanges);
- 12 international telegraphic transfers totalling approximately $5,893,002;
- two international telegraphic transfers totalling approx. $693,002;
- 171 inbound domestic transfers totalling $33,981,790;
- 51 outbound domestic transfers totalling $20,117,556;
- 30 transfers to Customer 5's Crown Melbourne DAB account totalling $29,784,433; and
- 27 transfers from Customer 5's Crown Melbourne DAB account totalling $27,530,933.

Customer 5 engaged in the following transactions at Crown Perth between 2014 and 2020 (SMR dated 2 July 2021):

- 47 sub-threshold cash deposits totalling $85,076;

- 12 sub-threshold cash withdrawals totalling $26,959;
- 34 threshold cash-ins (across his deposit account, direct cashier or table exchanges) totalling $1,497,973;
- 29 threshold cash-outs totalling $3,008,986 (either from his deposit account or direct cashier exchanges);
- 48 domestic transfers received totalling $21,935,726;
- 29 domestic transfers conducted totalling $9,026,538;
- nine other transfers totalling $6,239,386 to Customer 5's Crown Perth DAB account;
- 11 other transfers totalling $4,507,852 from Customer 5's Crown Perth DAB account; and
- one cheque was deposited into Customer 5's Crown Perth DAB account for $21,750.

In October 2021 an independent auditor identified that Customer 5 had run 155 junket programs between 2014 and 2020, for a total of 488 key players. The independent auditor made the following findings with respect to Customer 5's transactions, which were indicative of ML/TF typologies: see paragraph 24:

- Customer 5's transaction history at Crown displayed typologies of quick turnover of funds (without betting) and structuring;
- in relation to structuring, the independent auditor noted that one instance of potential structuring that was identified occurred between 14 and 17 March 2016 consisting of 13 potentially structured transactions with a total value of $111,000;
- in relation to the quick turnover of funds (without betting), the independent auditor noted that there were 11 instances of quick turnovers that occurred between 6 August 2014 and 20 August 2019 with a total of $2,495,023 deposited and $4,409,045 withdrawn through Customer 5's DAB account and safekeeping accounts;
- Customer 5 regularly received funds from third parties matched to Crown patrons as well as non-patrons;
- of the Crown patrons who sent funds to Customer 5's DAB account across 143 transactions:
    - transactions related to three patrons comprised 49.7% of the transactions and 54.8% of the total value of all the payments to/from this cohort;
    - 101 transactions with a net value of $23,208,990 were linked to a patron who was not a key player on Customer 5's junket, compared to 42 transactions for a net value of $1,873,005 received from registered key players on Customer 5's junket;

- of the non-Crown patron individuals who sent funds to Customer 5's DAB account across 157 transactions:
    - 126 transactions did not contain details of the country of residence where the third party was located; and
    - one individual sent $6,558,000 between 2014 and 2016 to Customer 5, and the individual shared the same home address as Customer 5 and was also a shareholder and director in the same company as Customer 5;
- analysis of the financial transactions against gaming data for Customer 5's junket did not disclose any obvious links, meaning there was no obvious explanation for most of the transactions;
- of the 61 SMRs related to Customer 5, 21 SMRs dealt with telegraphic transfers from individuals who were not key players on Customer 5's junket, 32 SMRs related to junket key players on the junket programs recording win/losses on their gaming despite not recording any individual rated gaming activity;
- Customer 5 was the son of another patron who was a person of interest for law enforcement on six occasions, including for money-laundering;
- Customer 5 was the subject of law enforcement enquiries on two occasions in 2017 in relation to the origin of cash presented in plastic bags; and
- Customer 5 was noted by Crown to be affiliated with a group of junket operators who were involved in illicit funds transfers.

Ongoing customer due diligence

872. On and from 1 March 2016, on multiple occasions, the provision of designated services to Customer 5 by Crown Melbourne and Crown Perth raised red flags reflective of higher ML/TF risks as a result of Customer 5's junket activity.

Particulars

See paragraph 477.

Total junket activity

Between 2016 and 2020, Crown Melbourne recorded that gaming activity on junket programs run by Customer 5 at Crown Melbourne involved buy-in of $196,862,650, losses of $36,152,670 and turnover of $1,555,931,565.

Between 2016 and 2020, Crown Perth recorded that gaming activity on junket programs run by Customer 5 at Crown Perth involved buy-in of $135,088,700, losses of $4,763,272 and turnover of $606,435,633.

Junket activity in 2016

In 2016, Crown Melbourne recorded that gaming activity on junket programs run by Customer 5 at Crown Melbourne involved buy-in of $37,416,960, losses of $9,836,105, and turnover of $395,411,775.

Between 16 March 2016 and 23 November 2016, Crown Melbourne formed suspicions with respect to high losses noted for 12 key players under Customer 5's junkets at Crown Melbourne, totaling $3,603,590: SMRs dated 16 March 2016, 30 May 2016, 12 July 2016, 8 September 2016, 17 October 2016 and 23 November 2016.

In 2016, Crown Perth recorded that gaming activity on junket programs run by Customer 5 at Crown Perth involved buy-in of $20,983,000, wins of $299,825, and turnover of $160,072,300.

Junket activity in 2017

In 2017, Crown Melbourne recorded that gaming activity on junket programs run by Customer 5 at Crown Melbourne involved buy-in of $43,456,270, losses of $8,760,345, and turnover of $419,151,200.

Between 16 January 2017 and 3 November 2017, Crown Melbourne formed suspicions with respect to high losses in the amount of $3,469,080 noted for the key players under Customer 5's junkets at Crown Melbourne: SMRs dated 16 January 2017, 1 May 2017, 11 July 2017, 11 September 2017 and 3 November 2017.

In 2017, Crown Perth recorded that gaming activity on junket programs run by Customer 5 at Crown Perth involved buy-in of $35,707,150, losses of $1,467,685, and turnover of $148,641,400.

Junket activity in 2018

In 2018, Crown Melbourne recorded that gaming activity on junket programs run by Customer 5 at Crown Melbourne in 2018 involved buy-in of $44,293,710, losses of $12,910,320, and turnover of $285,822,500.

Between 8 January 2018 and 29 August 2018, Crown Melbourne formed suspicions with respect to high losses in the amount of $12,004,910 noted for the key players under Customer 5's junkets at Crown Melbourne: SMRs dated 8 January 2018, 9 February 2018, 22 June 2018 and 29 August 2018.

In 2018, Crown Perth recorded that gaming activity on junket programs run by Customer 5 at Crown Perth in 2018 involved buy-in of $26,321,000, wins of $280,045, and turnover of $65,024,600.

Junket activity in 2019

In 2019, Crown Melbourne recorded that gaming activity on junket programs run by Customer 5 at Crown Melbourne involved buy-in of $63,193,310, losses of $3,544,650, and turnover of $413,820,090.

In 2019, Crown Perth recorded that gaming activity on junket programs run by Customer 5 at Crown Perth involved buy-in of $44,801,050, losses of $1,263,062, and turnover of $183,516,883.

Junket activity in 2020

In 2020, Crown Melbourne recorded that gaming activity on junket programs run by Customer 5 at Crown Melbourne involved buy-in of $8,502,400, wins of $1,101,250, and turnover of $41,726,000.

In 2020, Crown Perth recorded that gaming activity on junket programs run by Customer 5 at Crown Perth involved buy-in of $7,276,500, losses of $1,452,655, and turnover of $49,180,450.

Between 2016 and 2020, Crown regularly reapproved a standing credit line of $5,000,000 for Customer 5's junket on a monthly basis for use at Crown Melbourne and Crown Perth.

873. On and from 1 March 2016, on multiple occasions, the provision of designated services to Customer 5 by Crown Melbourne and Crown Perth raised red flags reflective of higher ML/TF risks as a result of unusual transactions and patterns of transactions involving Customer 5 and his junket representatives, key players and third parties which had no apparent economic or visible lawful purpose.

Particulars

See paragraphs 420ff, 450, 451,456ff and 491.

Unusual transactions and patterns of transactions in 2016

On 2 March 2016 and 3 March 2016, two large telegraphic transfers of foreign currency were deposited to Customer 5's DAB account at Crown Melbourne from a third party: SMR dated 3 March 2016.

On 15 March 2016, two telegraphic transfers of $12,000 and $50,000 from a third party were deposited to Customer 5's DAB account at Crown Melbourne. Later that day, a further two telegraphic transfers of $50,000 and $50,000 from a third party were attributed to Customer 5's DAB account at Crown Melbourne.

From 14 to 17 March 2016, Customer 5 was linked to transactions indicative of ML/TF typologies of structuring, including 13 payments into a Southbank account totalling $110,000, in the following amounts – $7,000, $8,000, $8,500, $9,000, $9,500, $8,000, $8,500, $6,400, $8,600, $9,000, $9,200, $9,500 and $9,800 – deposited at branches and ATMs of an Australian bank in metropolitan Sydney.

On 21 March 2016, six telegraphic transfers (totalling $72,313) were attributed to Customer 5's DAB account at Crown Melbourne from six third parties who were not key players under Customer 5's junkets: SMR dated 21 March 2016.

On 29 March 2016, six telegraphic transfers in amounts under $10,000 totalling $52,500 were deposited into a Crown Melbourne held account at various branches of an Australian bank around

Sydney and attributed to Customer 5's DAB account at Crown Melbourne.

A further three telegraphic transfers totalling $11,000 were also attributed on 29 March 2016 to Customer 5's DAB account at Crown Melbourne from third parties: SMR dated 30 March 2016.

In July 2016, Customer 5's junket representatives engaged in unusual cash transactions which were not supported by gameplay at Crown Perth, including:

- on 6 July 2016, one of Customer 5's junket representatives made an exchange of chips for $10,000 cash by in circumstances where the patron has no recorded play to support the cash-out: SMR dated 8 July 2016; and
- on 13 July 2016, one of Customer 5's junket representatives deposited $599,150 in cash into Customer 5's safekeeping account: SMR dated 20 July 2016.

Between 8 August 2016 and 9 August 2016, 4 telegraphic transfers totalling $995,000 were deposited into Customer 5's DAB account at Crown Melbourne from a third party, who was not a key player on Customer 5's junket: SMR dated 10 August 2016.

On 5 September 2016, Customer 5 engaged in transactions indicative of ML/TF typologies involving quick turnover of funds (without betting) at Crown Perth, depositing $176,000, $80,000 and $69,023 by telegraphic transfer, then withdrawing $585,000 from his DAB account by telegraphic transfer the following day.

Unusual transactions and patterns of transactions in 2017

On 5 January 2017, a telegraphic transfer of $22,000 was deposited into Customer 5's DAB account at Crown Melbourne from a third party, who was not a key player on Customer 5's junket: SMR dated 6 January 2017.

On 5 January 2017, a cash transaction of $65,000 with the descriptor "AD" was transacted through Customer 5's Crown Melbourne DAB account.

On 12 January 2017, a telegraphic transfer of $240,000 was deposited into Customer 5's DAB account at Crown Melbourne from a third party, Person 10: SMR dated 13 January 2017.

On 18 April 2017, a telegraphic transfer of $500,000 was deposited into Customer 5's DAB account at Crown Melbourne from a third party, Person 38, who was not a current key player on Customer 5's junket: SMR dated 19 April 2017.

On 28 April 2017, $5,000,000 was transacted through Customer 5's DAB account, using the descriptor "REDEMPTION".

On 5 June 2017, a telegraphic transfer of $673,700 was deposited to Customer 5's DAB account at Crown Melbourne from a third party,

who was not a key player on Customer 5's junket, but had been a patron at Crown Melbourne, with suspicious losses of $98,500 in 2015 and $384,000 in 2014: SMR dated 6 June 2017.

On 1 July 2017, a telegraphic transfer of $60,000 on 1 July 2017 was withdrawn from Customer 5's DAB account and sent to a key player on Customer 5's junket, which did not correspond to her recorded play on the junket program, in which she lost $3,450: SMR dated 14 July 2017.

On 20 July 2017, a telegraphic transfer of $50,000 was deposited into Customer 5's DAB account at Crown Melbourne from a third party, who was not a current key player on Customer 5's junket: SMR dated 21 July 2017.

On 22 July 2017, two telegraphic transfers totalling $102,000 were deposited into Customer 5's DAB account at Crown Melbourne from a third party, who was not a current key player on Customer 5's junket: SMR dated 24 July 2017.

On 19 August 2017, a telegraphic transfer of $400,000 was deposited into Customer 5's DAB account at Crown Melbourne from another Australian casino.

On 2 September 2017, a player who Crown understood was a guest of Customer 5 exchanged chips for $11,000 cash in circumstances where the player had not played at Crown Melbourne since 31 August 2017: SMR dated 4 September 2017.

On 26 September 2017, two telegraphic transfers totalling $425,395 were deposited into Customer 5's DAB account at Crown Melbourne from a third party, Person 34, who was not a current key player on Customer 5's junket: SMR dated 27 September 2017.

Between August and November 2017, Customer 5's junket representative engaged in unusual cash transactions which was reported to a law enforcement agency by Crown Melbourne:

- on 18 August 2017, Customer 5's junket representative presented $500,000 in cash (which, when counted, ended up being $498,950 made up of $29,200 in $100 notes, $462,050 in $50 notes, $7,020 in $20 notes, and $680 in $10 notes) and requested gaming chips. The junket representative claimed that the funds had come from a previous key player who had played on a program in June/July 2017, but did not know where the player had got the funds: SMR dated 21 August 2017;
- on 18 October 2017, Customer 5's junket representative presented $140,000 in $50 notes and $10,000 in $100 notes and requested gaming chips, in the form of a chip purchase voucher: SMR dated 19 October 2018;
- on 7 November 2017, Customer 5's junket representative presented 3 plastic bags of cash, asked for them to be deposited into Customer 5's DAB account, advised the amount was

$319,000 but noted he did not know the breakdown of cash. When asked where the cash came from, the representative advised he had attended Customer 5's home to collect it. When questioned further he changed his mind and advised that he had collected it from a family member of Customer 5 in the food court outside of Crown. The cash was presented in a fashion that appeared as though it had not been issued by a cash dealer, bank or casino. When counted, poor quality counterfeit notes were discovered, with the ink coming off as they were being touched and handled. The actual cash received was $319,020, $60,800 of which was presented in $100 notes, $244,800 of which was presented in $50 notes, and the remainder in $20 and $10 notes (the confirmed counterfeit amount was $4,500 and a further $150 was suspected to be counterfeit). The representative was taken to a law enforcement agency and the cash was provided to the agency: SMR dated 8 November 2017; and

- the following day, on 8 November 2017, Customer 5's junket representative presented the cash that had been taken to a law enforcement agency the previous day, in the law enforcement agency's evidence bags, and requested the funds be deposited into Customer 5's DAB account. The actual cash received was $314,070 (comprised of $55,900 in $100 notes, $244,750 in $50 notes, $13,360 in $20 notes and $60 in $10 notes), including some counterfeit notes. The total amount deposited into Customer 5's DAB account was $313,520: SMR dated 9 November 2017.

On 20 December 2017, a telegraphic transfer of $84,857 was deposited into Customer 5's DAB account at Crown Melbourne from a third party, Person 34: SMR dated 22 December 2017.

Unusual transactions and patterns of transactions in 2018

On 5 January 2018, a telegraphic transfer of $127,156 from a third party, Person 34, was deposited into Customer 5's DAB account at Crown Melbourne.

On 12 February 2018, Customer 5 engaged in transactions indicative of ML/TF typologies involving quick turnover of funds (without betting), by depositing $20,000 by telegraphic transfer, then withdrawing $306,000 from his DAB account by telegraphic transfer on the same day.

On 20 July 2018, Crown Melbourne processed a telegraphic transfer of $500,000 from Customer 5's Crown Melbourne DAB account to a third party, Person 38.

On 24 July 2018, two telegraphic transactions of $260,000 and $240,000 were deposited into Customer 5's DAB account at Crown Melbourne from a third party, Person 34, on 24 July 2018.

On 11 December 2018, a telegraphic transfer of $500,000 was deposited into Customer 5's DAB account at Crown Melbourne from a third party, Person 38, who were not key players on any of Customer 5's junkets: SMR dated 14 December 2018.

On 3 December 2018, Customer 5 engaged in transactions indicative of ML/TF typologies involving quick turnover of funds (without betting), by depositing $50,000 by telegraphic transfer, then withdrawing $270,000 from his DAB account by telegraphic transfer on the same day.

Unusual transactions and patterns of transactions in 2019

On 11 January 2019, a telegraphic transfer of $605,310 was deposited into Customer 5's DAB account at Crown Melbourne from a third party, who were not key players on any of Customer 5's junkets: SMR dated 14 January 2019.

On 1 March 2019, Customer 5 engaged in transactions indicative of ML/TF typologies involving quick turnover of funds (without betting), by depositing $200,000 by telegraphic transfer, then withdrawing $200,000 from his DAB account by telegraphic transfer on the same day.

On 13 April 2019, a key player on Customer 5's junket sought to exchange chips for $12,000 cash when the player had not played since 29 March 2019: SMR dated 15 April 2019.

On 25 June 2019, Customer 5 engaged in transactions indicative of ML/TF typologies involving quick turnover of funds (without betting), by depositing $700,000 by telegraphic transfer, then withdrawing $1,111,270 from his DAB account by telegraphic transfer on the same day, then a further $5,000 the following day in cash.

On 13 July 2019, Customer 5 engaged in transactions indicative of ML/TF typologies involving quick turnover of funds (without betting), by depositing $85,000 and $200,000 by telegraphic transfer, then withdrawing $200,000 from his DAB account by telegraphic transfer on the same day.

On 20 August 2019, Customer 5 engaged in transactions indicative of ML/TF typologies involving quick turnover of funds (without betting) at Crown Perth, by depositing $150,000 by telegraphic transfer, then withdrawing $150,000 from his DAB account in cash on the same day.

On 26 August 2019, Customer 5 sought approval from Crown management to telegraphic transfer $287,868 from his safekeeping account (which held $1,260,421 at that date), to redeem a junket 'CCF' at an overseas casino. The Group General Manager – AML requested further information to understand the origin of the funds in safekeeping, following which investigations revealed that the funds were transferred into Customer 5's DAB account by a key player (Customer 50) as front money for his play under Customer 5's junket

in July 2019. The key player lost $669,000 during the junket, such that Customer 5 would be entitled to that proportion of the front money.

On 25 October 2019, junket operator, Person 36, transferred $800,000 from his Crown Melbourne DAB account to Customer 5's DAB account, in circumstances where neither junket operator was noted as a key player under the other's junket programs: SMR dated 28 October 2019.

On 23 December 2019, a patron requested Crown Melbourne arrange a telegraphic transfer of $500,000 from his Crown Perth DAB account to Customer 5's DAB account at Crown Melbourne. The patron was not a key player under Customer 5's junket in Crown Melbourne, but Crown staff were informed that the patron owed Customer 5 a debt from playing under Customer 5's junket in a foreign country.

On 26 December 2019, a series of transactions involving Customer 5's DAB account occurred as follows:

- a key player under another junket operator's program requested settlement of the junket program (under which he was showing a win of $905,200) in cash, rather than a cheque or bank transfer;
- Cage staff provided the funds in cash to the junket representative;
- later in the evening, Customer 5's junket representative approached the desk with the bags of cash provided to the previous junket and requested the cash be deposited into Customer 5's DAB account;
- Cage staff declined to accept the full amount, due to the daily deposit limit of $300,000;
- when Cage staff asked why the funds were not directly transferred to Customer 5's DAB account at the point of settlement, the junket representative stated that this was the way the key player wanted to do it;
- the key player was a foreign PEP: SMR dated 27 December 2019.

2020

On 24 December 2019, a telegraphic transfer of $500,000 from the Crown Perth DAB account of a patron (Person 29) was deposited in Customer 5's Crown Melbourne DAB account: SMR dated 1 January 2020 (which noted that Crown staff stated that Person 29 owed Customer 5 $500,000 as he was a key player on Customer 5's junket program in a foreign country, but otherwise did not have any information about the debt to Customer 5 and that Person 29 was an inactive foreign PEP due to his role as a former politician).

874. On and from 1 March 2016, the provision of designated services to Customer 5 by Crown Melbourne and Crown Perth raised red flags reflective of higher ML/TF risks as a result of

unusual transactions involving foreign remittance service providers including the Company 10 deposit service: see paragraphs 332ff and 359ff.

Particulars

Unusual transactions involving foreign remittance service providers in 2016

On 24 August 2016, a patron requested Crown Perth transfer $50,000 from his Crown Perth DAB account to Person 56's Crown Perth DAB account. On 27 August 2016, Person 56 then transferred $20,000 to Customer 5's DAB account and $2,000 to another Crown Perth patron's DAB account: SMR dated 31 August 2016.

Unusual transactions involving foreign remittance service providers in 2017

On 20 September 2017, a telegraphic transfer of $46,356 was deposited for the benefit of Customer 5 in a Southbank account from a third party, Person 10, with the description "REF 2017091900008072 /INV/PURCHASING GOODS /INV/2271376" with a note stating that the funds were to be for the purpose of gaming. Person 10 was an employee of Person 56, and that the funds were used to repay Customer 5's credit facility: SMR dated 3 November 2021.

Un*usual transactions involving foreign remittance service providers* ***in*** *2018*

Between 11 and 19 January 2018, eight telegraphic transfers totalling $1,999,840 were deposited by an overseas money changer (Company 9) into a Southbank account which were used for front money, deposited into Customer 5's DAB account as well as the repayment of credit owed to Customer 5.

On 8 February 2018, four telegraphic transfers totalling $1,000,000 were deposited into Customer 5's DAB account at Crown Melbourne from a third party company, Company 9, which Crown understood was a money changer, but did not appear on the foreign country's money changer website: SMR dated 9 February 2018.

Between 20 June 2018 and 25 June 2018, remittance payments from Person 56 were distributed using Crown Melbourne's DAB accounts to a number of patrons, including to Customer 5, as follows:

- on 20 June 2018, a Crown patron transferred $5,248,366 to Person 56's DAB account; and
- Person 56 distributed these funds to three different patrons, including to Customer 5's Crown Melbourne DAB account on 26 June 2018 ($800,000, $100,095, $100,000) and on 29 June 2018 ($800,000).

Between 1 November 2018 and 14 November 2018, Crown Perth agreed to accept repayment of a junket-related debt owed to it by way of offsetting arrangements involving Customer 5 and another junket operator, Person 8, who Crown Perth knew was playing

alongside Customer 5 through the Company 10 deposit service in which:

- the junket operator deposited $500,000 with Company 10;
- Crown Perth made an agreement with Company 10 to release funds, against the funds held by Company 10, for Person 8 to use as front money for a junket program;
- Person 8 recorded losses of $497,000, however had $447,518 in his Crown Perth DAB accumulated by chip deposits during the junket program;
- Company 10 transferred $52,482 to Crown Perth taking Person 8's DAB account balance to $500,000; and
- Company 10 subsequently released $500,000 to Person 8 in South East Asia: SMR dated 20 November 2018.

See paragraphs 332ff and 359ff.

875. From November 2018, the provision of designated services to Customer 5 by Crown Perth raised red flags reflective of higher ML/TF risks arising from suspicious transactions on the Crown Perth HKD currency account.

Particulars

See paragraph 447.

Between 4 and 5 November 2018, five HKD transactions totalling HKD2,955,000 (approx. AUD$509,196.57) for the benefit of Customer 5 were transacted on the Crown Perth HKD currency account, in circumstances where it was not possible to establish a link between the HKD transactions and any junket program run by Customer 5: SMR dated 2 July 2021.

On 1 November 2019, HKD340,000 (approx. AUD$61,151.08) for the benefit of Customer 5 were transacted on the Crown Perth HKD account, in circumstances where it was not possible to establish a link between the HKD transactions and any junket program run by Customer 5: SMR dated 2 July 2021.

876. At no time did Crown Melbourne or Crown Perth undertake appropriate risk-based customer due diligence with respect to Customer 5 with a view to identifying, mitigating and managing the ML/TF risks posed by the provision of designated services on and from 1 March 2016.

a. At no time did Crown Melbourne or Crown Perth take appropriate steps to understand whether Customer 5's source of wealth/funds was legitimate.

b. At no time did Crown Melbourne or Crown Perth take appropriate steps to identify or analyse the ML/TF risks of Customer 5's transactions or to consider whether they had a lawful purpose.

c. At no time did Crown Melbourne or Crown Perth give appropriate consideration to whether large and high risk transactions should be processed.

d. On the one occasion prior to June 2021 that senior management considered whether to continue the business relationship with Customer 5 in January 2017, senior

management failed to give adequate consideration to whether the ML/TF risks posed by Customer 5 were within Crown Melbourne or Crown Perth's risk appetite: see paragraph 668ff.

Particulars

Section 36(1)(a) of the Act.

The due diligence steps taken with respect to Customer 5 included:

Database searches

Between September 2016 and December 2016, Crown also performed screenings on Customer 5's name on risk intelligence and company databases. Further risk intelligence searches were performed in January, July and October 2018.

On 15 July 2020, Crown Melbourne performed a search in its SEER surveillance database, which only noted incidents where counterfeit currency was discovered during buy-ins by Customer 5's key players.

Wealth reports

On 12 May 2016, Crown obtained a wealth report on Customer 5, which reported that Customer 5 was affiliated with an overseas junket operator and its affiliate which was allegedly involved in moving money around foreign jurisdictions.

Updated wealth reports were obtained on 10 January 2017, 28 November 2018, and July 2020.

Junket profiles

By 19 January 2017, the Credit control team prepared a junket profile on Customer 5, which incorporated findings from searches performed in late 2016 and noted that Customer 5's junkets had turned over $1,700,000,000 since 2014 and that Customer 5's family had a 20 year relationship with Crown.

On 12 April 2017, 18 December 2018, 18 November 2019, 22 July 2020, the Credit control team updated Customer 5's junket profile and recommended that Crown continue to conduct business with Customer 5.

Senior management consideration

On 19 January 2017, a VIP Operations meeting attended by the Chief Executive Officer (Crown Resorts), Executive General Manager, (Legal & Regulatory Services), a Crown Resorts director, Group General Counsel (Crown Resorts), Chief Executive Officer (Australian Resorts), Senior Vice President (International Business) and Group General Manager (International Business Operations), considered Customer 5's junket profile.

In July 2017, the AML/CTF Compliance Officer meeting determined to remove the SYCO alert monitoring in respect of Customer 5 after

reviewing his risk information but retain Customer 5's moderate risk rating.

During June and July 2021, Crown Melbourne and Crown Perth performed an analysis of Customer 5's financial and gaming activity on junket programs run by Customer 5 and identified suspicious patterns of transactions involving ML/TF typologies and large scale transactions which had no apparent economic or visible lawful purpose.

On 22 June 2021, Crown Melbourne issued a WOL in respect of Customer 5.

On 22 June 2021, Crown Perth issued an NRL in respect of Customer 5.

Prior to June 2021, none of these steps were proportionate to the ML/TF risks reasonably posed by Customer 5 on and from 1 March 2016.

Enhanced customer due diligence

877. Having formed a suspicion for the purposes of s41 of the Act, Crown Melbourne gave the AUSTRAC CEO SMRs with respect to Customer 5 on 42 occasions listed in Schedule 3.5.

Particulars

The SMRs reported:

- patterns of suspicions relating to key player wins and losses under Customer 5's junkets;
- unusual activity by a junket representative of Customer 5's junket;
- transactions with unrelated third parties; and
- transactions indicative of ML/TF typologies.

See particulars to paragraphs 871, 872, 873 and 874.

878. On each occasion that Crown Melbourne formed a suspicion with respect to Customer 5 for the purposes of s41 of the Act, it was required to apply its ECDD program to Customer 5.

Particulars

Rule 15.9(3) of the Rules.

879. Crown Melbourne did not carry out appropriate risk-based ECDD measures with respect to Customer 5 on each occasion that Crown Melbourne formed a suspicion with respect to Customer 5 for the purposes of s41 of the Act.

a. There are no records of ECDD being conducted after giving the AUSTRAC CEO any SMRs before the 1 July 2021 SMR: see paragraphs 664 and 685.

b. Appropriate risk-based steps were not taken to obtain or analyse Customer 5's source of wealth/funds: see paragraph 667.

c. Appropriate risk-based steps were not taken to analyse and monitor Customer 5's transactions – both past and future – including to understand their economic purpose: see paragraphs 590 and 666.

d. On the one occasion prior to June 2021 that senior management considered whether to continue the business relationship with Customer 5 in January 2017, senior management failed to give adequate consideration to whether the ML/TF risks posed by Customer 5 was within Crown Melbourne's risk appetite: see paragraph 668ff.

Particulars

Rule 15.9(3), 15.10(1)(c), (d), (2), (5) and (6) of the Rules.

On 22 June 2021, Crown Melbourne issued a WOL in respect of Customer 5.

After giving the AUSTRAC CEO the 1 July 2021 SMR, Crown Melbourne undertook a detailed lookback of Customer 5's gaming activities: see paragraph 871.

See the particulars to paragraph 876.

880. Having formed a suspicion for the purposes of s41 of the Act, Crown Perth gave the AUSTRAC CEO SMRs with respect to Customer 5 on:

a. 8 July 2016;

b. 20 July 2016;

c. 31 August 2016;

d. 14 July 2017;

e. 4 September 2017;

f. 20 November 2018;

g. 15 April 2019;

h. 1 January 2020; and

i. 2 July 2021.

Particulars

The SMRs reported:

- transactions related to debt settlement or offsets not related to Customer 5's junket;
- transactions with unrelated third parties; and
- transactions indicative of ML/TF typologies.

See particulars to paragraphs 871, 872, 873 and 874.

881. On each occasion that Crown Perth formed a suspicion with respect to Customer 5 for the purposes of s41 of the Act, it was required to apply its ECDD program to Customer 5.

Particulars

Rule 15.9(3) of the Rules.

882. Crown Perth did not carry out appropriate risk-based ECDD measures with respect to Customer 5 on each occasion that Crown Perth formed a suspicion with respect to Customer 5 for the purposes of s41 of the Act.

a. There are no records of ECDD being conducted after giving the AUSTRAC CEO SMRs on 8 July 2016, 20 July 2016, 31 August 2016, 14 July 2017, 4 September 2017, 20 November 2018, 15 April 2019, and 1 January 2020: see paragraphs 664 and 685.

b. Appropriate risk-based steps were not taken to obtain or analyse information about Customer 5's source of wealth/funds: see paragraph 667.

c. Appropriate risk-based steps were not taken to analyse and monitor Customer 5's transactions – both past and future – including to understand their economic purpose: see paragraphs 590 and 666.

d. On the one occasion prior to June 2021 that senior management considered whether to continue the business relationship with Customer 5 in January 2017, senior management failed to give adequate consideration to whether the ML/TF risks posed by Customer 5 was within Crown Perth's risk appetite.

Particulars

Rule 15.9(3), rule 15.10(1)(c), (d), (2), (5) and (6) of the Rules.

On 22 June 2021, Crown Perth issued an NRL in respect of Customer 5.

After giving the AUSTRAC CEO the 2 July 2021 SMR, Crown Perth undertook a detailed lookback of Customer 5's gaming activities: see paragraph 871.

See the particulars to paragraph 876.

883. By reason of the matters pleaded at paragraphs 856 to 882, on and from 1 March 2016, Crown Melbourne and Crown Perth:

a. did not monitor Customer 5 in relation to the provision of designated services, with a view to identifying, mitigating and managing the ML/TF risks reasonably faced; and

b. did not do so in accordance with rr15.5 and 15.9 of the Rules.

884. By reason of the matters pleaded at paragraph 883, Crown Melbourne and Crown Perth contravened s36(1) of the Act on and from 1 March 2016 to 22 June 2021 with respect to Customer 5.

Particulars

Section 36(1) of the Act is a civil penalty provision: s36(2) of the Act.

NEPTUNE JUNKET

885. At various times between 2008 to March 2020, Crown Melbourne and Crown Perth had a NONEGPRA with numerous junket operators who were part of a network of junket operators affiliated with the Neptune Group and Neptune Guangdong Group (**Neptune junket**), Person 3, Customer 6, Customer 7, Customer 8 and Customer 9.

Particulars

Crown Melbourne

On 1 July 2004, Crown Melbourne and Person 3 entered into a NONEGPRA. Person 3 operated junket programs at Crown Melbourne until approximately 2014.

On 3 February 2008, Crown Melbourne and Customer 6 entered into a NONEGPRA. Customer 6 operated junket programs at Crown Melbourne until March 2020.

On 6 October 2010, Crown Melbourne and Customer 8 entered into a NONEGPRA. Customer 8 operated junket programs at Crown Melbourne until December 2016.

On 30 May 2011, Crown Melbourne and Customer 9 entered into a NONEGPRA. Customer 9 operated junket programs at Crown Melbourne until 25 February 2020.

On 29 June 2015, Crown Melbourne and Customer 7 entered into a NONEGPRA. Customer 7 operated junket programs at Crown Melbourne until 2016.

Crown Perth

On 25 September 2014, Crown Perth and Customer 6 entered into a NONEGPRA. Customer 6 operated junket programs at Crown Perth until at least May 2018.

On 16 July 2012, Crown Perth and Customer 8 entered into a NONEGPRA. Customer 8 operated junket programs at Crown Perth until November 2016.

On 25 July 2011, Crown Perth and Customer 9 entered into a NONEGRA. Customer 9 operated junket programs at Crown Perth until November 2015.

On 29 June 2015, Crown Perth and Customer 7 entered into a NONEGPRA. Customer 7 operated junket programs at Crown Perth until approximately late 2015.

886. On and from 1 March 2016, the provision of designated services by Crown Melbourne and Crown Perth to junket operators who were part of the Neptune junket posed higher ML/TF risks due to the involvement of Person 3, Person 55 and Customer 6 who were ultimate beneficial owners of the Neptune junket with financial interests in its operations.

a. By at least October 2013:

i. Crown Melbourne and Crown Perth were aware that the ILGA had raised concerns with another Australian casino's association with the Neptune junket during its casino license review.

ii. Crown Melbourne and Crown Perth were aware that Person 3 and Person 55 were the principal partners of the Neptune junket, with Customer 8 and Customer 9 acting only as the front men for the Neptune junket.

b. By 1 March 2016, Crown Melbourne and Crown Perth were aware that a principal partner and ultimate beneficial owner of the Neptune junket, Person 3 had suspected links to organised crime, was linked to alleged bribery, money laundering, and an illegal underground banking network for corrupt officials and businesses to launder money, and was a foreign PEP (see paragraphs 118 and 663).

c. By 1 March 2016, Crown Melbourne and Crown Perth were aware that a principal partner and ultimate beneficial owner of the Neptune junket, Person 55, was allegedly the leader of an organised crime syndicate, was the mastermind of a 2009 conspiracy to murder a casino dealer at an overseas casino (at a time when Person 55 was in charge of VIP rooms at the casino), had his assets frozen in 2014, was later arrested in 2015 for charges of money laundering up to HKD1,400,000,000 between 2004 and 2010, and was connected to associates with links to organised crime.

d. By 1 March 2016, Crown Melbourne and Crown Perth were aware that an ultimate beneficial owner of the Neptune junket, Customer 6, had been arrested in 2012 on the basis of allegations that he had engaged in money laundering and underground bank activities and had made a suspicious transfer at an overseas casino.

887. At all relevant times, the provision of designated services by Crown Melbourne and Crown Perth to junket operators who were part of the Neptune junket posed higher ML/TF risks including because:

a. the table 3, s6 designated services provided to junket operators who were part of the Neptune junket involved high turnover at Crown Melbourne and Crown Perth:

i. between 2008 and 2020, the total turnover from recorded gaming activity on junket programs run by junket operators associated with the Neptune junket at Crown Melbourne and Crown Perth was $32,157,076,451, comprising:

– approximately $21,764,350,654 at Crown Melbourne; and

– approximately $10,392,725,797 at Crown Perth;

b. key players on junket programs run by the Neptune junket operators had high losses at Crown Melbourne and Crown Perth:

i. by 1 March 2016, total reported losses by key players on junket programs run by Customer 6, Customer 7, Customer 8 and Customer 9 amounted to $132,960,694 and, separately, HKD1,347,500; and

ii. on and from 1 March 2016, total reported losses by key players on junket programs run by Customer 6, Customer 7, Customer 8 and Customer 9 amounted to $160,719,049;

c. Neptune junket operators were involved in a number of large and unusual third party transactions:

i. by 1 March 2016, total reported incoming third party transactions involving Customer 6, Customer 7, Customer 8 and Customer 9 totalled approximately $10,076,428 and HKD119,829,840;

ii. by 1 March 2016, total reported outgoing third party transactions involving Customer 6, Customer 7, Customer 8 and Customer 9 totalled approximately $37,360,903 and HKD25,408,350;

iii. on and from 1 March 2016, total reported incoming third party transactions involving Customer 6, Customer 7, Customer 8 and Customer 9 totalled approximately $4,598,133 and HKD32,249,105; and

iv. on and from 1 March 2016, total reported outgoing third party transactions involving Customer 6, Customer 7, Customer 8 and Customer 9 totalled approximately $23,063,251.

Customer 6

888. Customer 6 was a customer of Crown Melbourne from at least 1 January 2006 to 20 November 2020.

889. From at least December 2006, Crown Melbourne provided Customer 6 with designated services within the meaning of table 1 and table 3, s6 of the Act.

890. From at least 3 February 2008 to 16 March 2020, Customer 6 received designated services as a junket operator at Crown Melbourne for the Neptune junket, as an independent junket operator and as a junket player.

Particulars to paragraphs 889 and 890

Crown Melbourne opened a DAB account and safekeeping account for Customer 6 on the following nine occasions:

- 1 July 2006 under an PID;
- 22 December 2015 under a second PID;
- 9 January 2016 under a third PID;
- 15 October 2017 under a fourth PID;
- 1 October 2018 under a fifth PID;
- 2 October 2018 under a sixth PID;
- 16 January 2019 under a seventh PID;
- 24 November 2019 under a eighth PID; and
- 24 November 2019 under a ninth PID.

On 3 February 2008, Crown Melbourne entered into a NONEGPRA with Customer 6 to operate junkets at Crown Melbourne. On 13 June 2019, Customer 6 entered into an updated NONEGPRA with Crown Melbourne.

On 22 April 2008, Crown Melbourne opened a credit facility for Customer 6 under his first PID. On 24 November 2020, Crown Melbourne closed Customer 6's credit facility.

Between 17 April 2016 and 17 March 2020, Customer 6 operated at least 107 junket programs at Crown Melbourne, including 41 under his first PID, 28 under his second PID, 17 under his third PID, 10 under his fourth PID, 6 under his fifth PID and 5 under his sixth PID. During this period, Customer 6 had 49 junket representatives.

Customer 6 received designated services as a junket player through his own junket programs and the Customer 7 junket as part of the Neptune junket (see paragraph 564ff), Suncity (see paragraph 521ff) and Meg-Star junkets (see paragraph 555ff).

On 20 November 2020, Crown Melbourne issued an indefinite WOL in respect of Customer 6.

On 20 January 2021, the Crown Resorts POI Committee considered Customer 6, who had come to the Committee's attention through the ILGA inquiry.

On 12 November 2021, Crown Melbourne closed each of Customer 6's DAB account and safekeeping accounts opened under the nine PIDs.

891. Customer 6 was a customer of Crown Perth from at least 26 September 2014 to 20 November 2020.

892. From at least 26 September 2014, Crown Perth provided Customer 6 with designated services within the meaning of table 1 and table 3, s6 of the Act.

893. From at least 26 September 2014, Customer 6 received designated services as a junket operator and as a junket player.

Particulars to paragraphs 892 and 893

On 25 September 2014, Crown Perth entered into a NONEGPRA with Customer 6 to operate junkets at Crown Perth. On 13 June 2019, Customer 6 entered into an updated NONEGPRA with Crown Melbourne.

Crown Perth opened a DAB account and safekeeping account for Customer 6 on the following occasions:

- 29 September 2014 under an initial PID;
- 3 May 2016 under a second PID; and
- 20 September 2019 under a third PID.

On 26 September 2014, Crown Perth opened a FAF for Customer 6. On 16 January 2019, Crown Perth opened an additional FAF for Customer 6 under a different PID. On 24 November 2020, Crown Perth closed both of Customer 6's FAFs.

Between 11 March 2016 and 22 October 2019, Customer 6 operated at least 20 junket programs at Crown Perth, including 16 under his first PID, four under his second PID and one under his third PID. During this period, Customer 6 had 17 unique junket representatives.

Customer 6 received designated services as a junket player through his own junket programs and under junkets run by other Neptune junket operators (Customer 7) and two other junket operators.

On 20 November 2020, Crown Perth issued an NRL with respect to Customer 6.

On 20 January 2021, the Crown Resorts POI Committee considered Customer 6, who had come to the Committee's attention through the ILGA inquiry, and noted that an NRL had already been issued to Customer 6.

The ML/TF risks posed by Customer 6

894. By 1 March 2016, higher ML/TF risks were indicated by the nature and purpose of Customer 6's business relationship with Crown Melbourne and Crown Perth as a junket operator linked to the Neptune junket, his connections to other junket operators and representatives associated with the Neptune junket, including ultimate beneficial owners Person 3 and Person 55, nature of the transactions he had been conducting, together with the suspicions Crown Melbourne and Crown Perth itself had formed with respect to Customer 6.

Particulars

Section 36(1)(a), (b) of the Act and Chapter 15 of the Rules.

Customer 6 was a junket operator and junket player. He received designated services through the channel of junket programs. This channel lacked transparency: see paragraph 477.

Links to Neptune junket

By 1 March 2016, Crown Melbourne was aware that Customer 6 was connected to the Neptune junket and, as a result, also connected to Person 3 and Person 55 who were the ultimate beneficial owners behind the junket: see paragraph 886.

In August 2014, Customer 6 had transferred $10,000,000 from his Crown Melbourne DAB account to the DAB account of another Neptune junket operator, Customer 9: SMR dated 21 August 2014.

On 18 July 2015, Customer 6 provided Crown with a joint letter of guarantee in support of a credit facility with a limit of AUD$250,000,000 to Customer 7, another junket operator associated with the Neptune junket.

Junket activity (Crown Melbourne)

By 1 March 2016, Customer 6 had operated approximately 34 junket programs at Crown Melbourne. Crown Melbourne recorded that the total turnover for those programs was $4,918,395,637, with losses of $53,884,350.

By 1 March 2016, Crown management approved numerous credit facilities for Customer 6's junkets prior to the junket programs in various amounts ranging from $6,000,000 to $25,000,000.

By 1 March 2016, Customer 6 owed large sums ($3,699,998) to Crown Melbourne. These debts were subsequently discharged.

Junket activity (Crown Perth)

By 30 June 2015, gaming activity on junket programs run by Customer 6 at Crown Perth involved turnover of $1,939,800,100 and wins of $31,977,215.

SMRs (Crown Melbourne)

By 1 March 2016, Crown Melbourne had given the AUSTRAC CEO 29 SMRs in relation to Customer 6. The SMRs reported:

- key player wins and losses (collectively total wins of $288,300 and total losses of $46,793,765 between February 2007 and January 2016);
- Customer 6's wins and losses as a junket player under other junket programs (collectively, total wins of $539,250 and total losses of $9,982,500 by Customer 6 between May 2009 and August 2015);
- transactions with unrelated third parties; and
- suspicious transactions, including:
  - on 27 September 2007, HKD3,500,000 in gaming chips belonging to Customer 6 which were being held overseas for a third party and were intended to be made available to at Crown Melbourne. The third party did not use these funds and instead presented a cheque for AUD$200,000: SMR dated 27 September 2007; and
  - on 12 October 2012, two large cash deposits totalling $150,000 were deposited by a third party, who is believed to be the son of Customer 6: SMR dated 12 October 2012.

SMRs (Crown Perth)

By 1 March 2016, Crown Perth gave the AUSTRAC CEO one SMR, which recorded:

- On 10 August 2015, Crown Perth sent $8,504,500 via telegraphic transfer from Customer 6's DAB account to another junket operator's account at Crown Melbourne; and
- On 14 August 2015, Crown Perth sent a second telegraphic transfer of $3,518,400 to another Neptune junket operator, Customer 8.

Due diligence

By 1 March 2016, the due diligence steps taken with respect to Customer 6 were as follows.

On 12 September 2014, Crown Perth performed a risk intelligence search on Customer 6.

On 7 January 2015 and 6 November 2015, Crown Melbourne performed risk intelligence searches which reported that Customer 6 had been detained overseas in 2012 for his alleged involvement in money-laundering.

On 2 July 2015, Crown Melbourne and Crown Perth obtained a wealth report on Customer 6, which reported on his business activities and alleged detention in 2012.

On 21 August 2015, following a request by Crown Aspinalls employees to provide due diligence records on patrons including Customer 6, the General Manager – Compliance (Crown Melbourne) stated that Crown Melbourne had reviewed the records and decided to continue to deal with the patrons, including Customer 6, on the basis that there was nothing official or substantive to support the negative material on them.

895. At all relevant times, Customer 6 should have been recognised by Crown Melbourne as a high risk customer for the reasons pleaded at paragraph 894.

Particulars

Section 36(1)(a), (b) of the Act and Chapter 15 of the Rules.

896. At all times on and from 1 March 2016, Customer 6 should have been recognised by Crown Melbourne as a high risk customer by reason of the matters pleaded at paragraphs 894, 901, 902, 903, 904, 905, 906 and 908.

Particulars

Section 36(1)(a), (b) of the Act and Chapter 15 of the Rules.

897. It was not until 20 January 2021 that Crown Melbourne rated Customer 6 high risk.

Particulars

On at least 9 occasions between 27 September 2007 and 12 October 2012, Crown Melbourne rated Customer 6 moderate risk.

On at least 56 occasions between 26 November 2011 and 28 February 2020, Crown Melbourne rated Customer 6 significant risk.

See paragraph 481.

898. As at 1 March 2016, Customer 6 should have been recognised by Crown Perth as a high risk customer for the reasons pleaded at paragraph 894.

Particulars

Section 36(1)(a), (b) of the Act and Chapter 15 of the Rules.

899. At all times on and from 1 March 2016, Customer 6 should have been recognised by Crown Perth as a high risk customer by reason of the matters pleaded at paragraphs 894, 901, 902, 903, 904, 905, 906 and 911.

Particulars

Section 36(1)(a), (b) of the Act and Chapter 15 of the Rules.

900. It was not until 20 January 2021 that Crown Perth rated Customer 6 high risk.

Particulars

On 27 September 2014, Crown Perth rated Customer 6 low risk.

On at least six occasions between 12 December 2014 and 2 October 2019, Crown Perth assessed Customer 6 moderate risk.

See paragraph 481.

901. On and from 1 March 2016, designated services provided to Customer 6 posed higher ML/TF risks including because the provision of designated services to Customer 6 involved a combination of the following factors:

a. Customer 6 was a junket operator associated with the Neptune junket;

b. Customer 6 was a junket player, including on junket programs run by Neptune junket operators;

c. at all times, Crown Melbourne was aware of Customer 6's connections to the Neptune junket and that he was an ultimate beneficial owner along with Person 3 and Person 55. This connection presented high ML/TF risks for the reasons set out at paragraph 886;

d. Customer 6 received high value financial services (table 1, s6) and gaming services (table 3, s6), through multiple junket programs: see paragraph 473ff;

e. Customer 6 was a junket operator who facilitated the provision of high value financial and gaming services (tables 1 and 3, s6) to key players on his junket programs: see paragraph 473ff;

f. Customer 6 was known at all times to be connected to other junket operators, including junket operators in respect of whom Crown Melbourne or Crown Perth had formed suspicions such as Customer 1, Customer 7, Customer 9 and Person 3;

g. designated services provided to Customer 6 lacked transparency as the services were provided through the channel of junket programs: see paragraph 477(e);

h. designated services provided to Customer 6 lacked transparency because he operated junket programs for both for the Neptune junket and as an independent junket operator;

i. the table 3, s6 designated services provided to Customer 6 involved high turnover;

j. designated services provided to Customer 6 involved large cross-border movements of funds: see paragraph 238(d);

k. large values were transferred to and from Customer 6's DAB account, and to and from other customers' DAB accounts, involving the provision by Crown Melbourne of designated services within the meaning of items 31 and 32, table 1, s6 of the Act: see paragraphs 411ff and 492;

l. large values were transferred to and from Customer 6's bank accounts and his DAB account, involving the provision by Crown Melbourne of designated services within the meaning of items 31 and 32, table 1, s6 of the Act: see paragraphs 411ff and 492;

m. on multiple occasions, Crown Melbourne made available the Crown private jet for Customer 6. There were inadequate controls on the carrying of large amounts of cash on Crown's private jets*:* see paragraphs 454 and 491(c);

n. at various times, Customer 6 had significant parked or dormant funds in his DAB accounts: see paragraph 252;

o. at various times, Customer 6 was provided with significant amounts of credit upon request, up to limits of AUD$50,000,000 or HKD100,000,000, including a standing credit line with a limit of $5,000,000 from November 2017, which was increased to $20,000,000 between April 2018 and March 2020: see paragraphs 280ff and 487;

p. these transactions took place against the background of:

i. by 1 March 2016, Crown Melbourne recorded turnover on junket programs operated by Customer 6 that exceeded $4,918,395,63;

ii. by 1 March 2016, Crown Perth recorded turnover on junket programs operated by Customer 6 that exceeded $1,939,800,100;

iii. 29 SMRs being given to the AUSTRAC CEO by Crown Melbourne and one SMR being given by Crown Perth by 1 March 2016;

q. on and from 1 March 2016, Crown Melbourne and Crown Perth were aware that Customer 6 had been detained in overseas for alleged involvement in money-laundering;

r. on November 2016 and February 2018, law enforcement made enquiries into funds linked to Customer 6; and

s. by reason of the matters pleaded at a. to r., and in light of his connections to the Neptune junket, there were real risks that Customer 6's source of wealth/funds were not legitimate.

Monitoring of Customer 6's transactions

902. At no time did Crown Melbourne or Crown Perth appropriately monitor Customer 6's transactions on a risk-basis.

Particulars

Section 36(1)(a), (b) of the Act and rules 15.4 to 15.8 of the Rules.

Crown Melbourne and Crown Perth was unable to monitor the ML/TF risks posed by Customer 6's transactions appropriately because they did not make and keep appropriate records of designated services provided to junket operators or junket players: see paragraphs 483ff.

Crown Melbourne and Crown Perth did not apply appropriate risk-based transaction monitoring to designated services provided to Customer 6: see paragraphs 590ff and 629 to 642 (designated services) and 643 to 649 (transactions facilitated through junkets).

Inadequate controls on Crown's private jets

Crown Melbourne provided Customer 6 with a Crown private junket at the junket's request to facilitate travel on:

- 5 May 2016, from Perth to Melbourne for 4 people;
- 7 May 2016, from Melbourne to an overseas country for 7 people;
- 26 June 2016, Melbourne to Sydney for 9 people;
- 20 August 2016, an overseas country to Perth for 3 people;
- 22 August 2016, Perth to Melbourne for 3 people; and
- 25 August 2016, Melbourne to an overseas country for 5 people.

On 6 February 2018, Customer 6, when entering Australia as a passenger on Crown's private jet, was discovered to be in possession

of $790,000 in undeclared cash over the threshold for declaration upon entry into Australia following a routine immigration and customs inspection. Crown Melbourne advised the law enforcement agency that Crown had been aware of the funds and understood it would be used to repay a junket operator's debt. The law enforcement agency did not confiscate the cash, which was subsequently taken to Crown and $785,000 was deposited by Customer 6 into the account of another junket operator, to repay a debt from his credit facility at Crown Melbourne: SMR dated 8 February 2018.

There were inadequate controls on the carrying of large amounts of cash on Crown's private jets: see paragraphs 454 and 491(c).

Lookback

Customer 6's transactions involved repeated transactions indicative of ML/TF typologies and vulnerabilities that were not detected prior to a 2021 lookback. Had appropriate risk-based transaction monitoring been applied, these transactions could have been identified earlier: see paragraph 686 and 687.

ML/TF typology – parking

Transactions involving Customer 6 were identified as indicative of the ML/TF typology of parking by an independent expert in 2021. As at 30 April 2021, Customer 6 had parked $2,319,735.56 in his safekeeping account. The funds were still parked in the account as at 18 June 2021. There had been no activity on the DAB or safekeeping accounts since 14 April 2020.

ML/TF typology – quick turnover of funds

In 2021, transactions involving Customer 6 were identified as indicative of the ML/TF typology of quick turnover of funds (without betting) by an independent auditor:

- on 3 December 2016, Customer 6 engaged in transactions in which $400,000 was deposited into Customer 6's DAB account by telegraphic transfer, then $400,000 was withdrawn from his DAB account by telegraphic transfer on the same day; and
- on 6 November 2019, Customer 6 engaged in transactions in which $250,000 was deposited into Customer 6's DAB account by telegraphic transfer. The following day, on 7 November 2019, $3,400,000 was withdrawn from his DAB account by telegraphic transfer.

Ongoing customer due diligence

903. On and from 1 March 2016, on multiple occasions, the provision of designated services to Customer 6 at Crown Melbourne and Crown Perth raised red flags reflective of higher ML/TF risks as a result of Customer 6's connections to the Neptune junket and its UBOs Person 3, Person 55 and Customer 6.

Particulars

Section 36(1)(a), (b) of the Act and Chapter 15 of the Rules.

By 1 March 2016, Crown Melbourne and Crown Perth were aware that Customer 6, along with Person 3 and Person 55 were the UBOs and controllers behind the Neptune junket operators at Crown, and had financial interests in the business of the Neptune junket.

See paragraph 886.

904. On and from 1 March 2016, on multiple occasions, the provision of designated services to Customer 6 by Crown Melbourne and Crown Perth raised red flags reflective of higher ML/TF risks arising from Customer 6's junket activity.

Particulars

See paragraph 477.

Junket activity in 2016

Crown Melbourne recorded gaming activity on junket programs run by Customer 6 at Crown Melbourne by the end of the 2016 financial year as having turnover of approximately $3,325,671,016, with losses of approximately $5,860,590. Commissions of approximately $5,539,604 were payable by Crown Melbourne to Customer 6.

Crown Perth recorded gaming activity on junket programs run by Customer 6 at Crown Perth by the end of the 2016 financial year as having turnover of approximately $1,136,204,176 with wins of approximately $36,026,842.

Between 2 March 2016 and 5 September 2016, Crown Melbourne had formed suspicions with respect to high losses noted for the key players under Customer 6's junket program at Crown Melbourne, giving the AUSTRAC CEO four SMRs that described losses by 10 key players under Customer 6's junkets totalling $29,679,585: SMR dated 2 March 2016, 29 June 2016, 8 July 2016 and 5 September 2016.

Between March 2016 and October 2016, Crown management regularly reapproved Customer 6's credit facility, up to limits between $20,000,000 and $51,000,000.

Junket activity in 2017

Crown Melbourne recorded gaming activity on junket programs run by Customer 6 at Crown Melbourne by the end of the 2017 financial year as having turnover of approximately $564,867,856, with losses of approximately $21,986,519. Commissions of approximately $15,573,533 were payable by Crown Melbourne to Customer 6.

Crown Perth recorded gaming activity on junket programs run by Customer 6 at Crown Perth by the end of the 2017 financial year as having turnover of approximately $120,740,000 with wins of approximately $8,427,139.

Between 6 February 2017 and 15 November 2017, Crown Melbourne had formed suspicions with respect to high losses noted for the key players under Customer 6's junket program, giving the AUSTRAC CEO five SMRs that described losses by 11 key players under Customer 6's junkets totalling $29,331,040: SMR dated 6 February 2017, 17 October 2017, 13 November 2017, 14 November 2017 and 15 November 2017.

Between 16 January 2017 and 13 October 2017, Crown management regularly reapproved Customer 6's credit facility, up to limits of HKD25,000,000 and HKD100,000,000 and AUD$5,000,000 and AUD$20,000,000.

By November 2017, Customer 6 had negotiated a standing 'walk-in' credit line with Crown management, which would be reviewed by Crown Melbourne on a monthly basis. In November and December 2017, Crown management reapproved Customer 6's credit limit of $5,000,000, as part of a monthly junket review.

On 20 December 2017, Crown approved credit of $50,000,000 on a 70/30 rebate for Customer 6's junket.

Customer 6's losses under Suncity junket in November 2017 (Crown Melbourne)

In November 2017, Customer 6 was a key player on a Suncity junket at Crown Melbourne. Over the course of the program, Customer 6 was noted to have lost $9,960,000. Losses noted for 8 other key players on the program totalled $5,465,130: SMR dated 2 November 2017.

Junket activity in 2018

Crown Melbourne recorded gaming activity on junket programs run by Customer 6 at Crown Melbourne by the end of the 2018 financial year as having turnover of approximately $3,653,513,110 with losses of approximately $24,516,095. Commissions of approximately $51,133,125 were payable by Crown Melbourne to Customer 6.

Crown Perth recorded gaming activity on junket programs run by Customer 6 at Crown Perth by the end of the 2018 financial year as having turnover of approximately $96,513,403 and wins of approximately $9,483,476.

Between 27 February 2018 and 17 July 2018, Crown Melbourne had formed suspicions with respect to the high losses noted for the key players under Customer 6's junket program, giving the AUSTRAC CEO 4 SMRs that described losses by 5 key players under Customer 6's junkets totalling $10,196,870: SMR dated 27 February 2018, 23 March 2018, 16 April 2018 and 17 July 2018.

In early 2018, Crown management approved Customer 6's credit facility up to limits of AUD$30,500,000 and AUD$50,000,000.

From April 2018, Crown management and Customer 6 agreed to increase Customer 6's standing 'walk-in' credit line from $5,000,000 to $20,000,000. This was reapproved by Crown management on a monthly basis between April 2018 and December 2018.

Junket activity in 2019

Crown Melbourne recorded gaming activity on junket programs run by Customer 6 at Crown Melbourne by the end of the 2019 financial year as having turnover of approximately $1,577,982,827 with losses of approximately $31,808,244. Commissions of approximately $12,413,964 were payable by Crown Melbourne to Customer 6.

Crown Perth recorded gaming activity on junket programs run by Customer 6 at Crown Perth by the end of the 2019 financial year as having turnover of approximately $283,455,078 with wins of approximately $4,103,484.

From February 2019, Crown management and Customer 6 agreed to increase Customer 6's standing credit limit to $30,000,000. However, this limit was dropped back down to $20,000,000, which was reapproved by Crown management on a monthly basis between March 2019 and December 2019.

Junket activity in 2020

By 2 March 2020, Crown Melbourne recorded gaming activity on junket programs run by Customer 6 at Crown Melbourne as having turnover of approximately $1,953,517,121 with losses of approximately $13,851,490. Commissions of $7,668,825 were payable by Crown Melbourne to Customer 6.

By 2 January 2020, Crown Perth recorded gaming activity on junket programs run by Customer 6 at Crown Perth as having turnover of approximately $76,744,700 with wins of approximately $1,236,433.

In early 2020, Customer 6 played as a key player on a junket program at Crown Melbourne. Over the course of the program, Customer 6 was noted to have lost $15,470,000. Two other key players on the same junket were noted with losses totalling $33,605,500: SMR dated 28 February 2020.

On 6 March 2020, Customer 6's $20,000,000 standing credit limit was reapproved as part of a monthly junket review.

905. On and from 1 March 2016, on multiple occasions, the provision of designated services to Customer 6 by Crown Melbourne and Crown Perth raised red flags reflective of higher ML/TF risks as a result of unusual transactions, including suspicious cash transactions, involving Customer 6 and his junket representatives and key players.

Particulars

See paragraphs 420ff, 450,451, 456ff and 491.

Unusual transactions and patterns of transactions in 2016

On 20 May 2016, a telegraphic transfer of HKD5,749,105 from a third party was deposited into Customer 6's DAB account: SMR dated 23 May 2016.

On 21 December 2016, Customer 6 arranged for the transfer of $4,000,000 from his Crown Perth DAB account to the Crown Melbourne DAB account of another junket operator, Customer 1: SMR dated 6 February 2017.

Unusual transactions and patterns of transactions in 2017

On 10 July 2017, Crown Melbourne processed a transfer of $100,000 from Customer 6's DAB account to another patron: SMR dated 11 July 2017.

On 24 December 2017, Customer 6's junket representative withdrew $600,000 in cash from Customer 6's DAB account and refused to answer when asked what the funds were for: SMR dated 27 December 2017.

On 31 December 2017, a telegraphic transfer of $28,174 from a third party was deposited into Customer 6's DAB account: SMR dated 2 January 2018.

Unusual transactions and patterns of transactions in 2018

On 19 February 2018, $100,000 was transferred from Customer 6's Crown Melbourne DAB account to another Crown patron, who was not noted as a key player under Customer 6's junket. The patron then withdrew the $100,000 in cash: SMR dated 20 February 2018.

On 2 March 2018, HKD26,500,000 was sent by Customer 6 to Crown Melbourne by telegraphic transfer. The transfer was intended to pay a third party's debt owed to Crown Aspinalls: see paragraphs 332ff and 375ff. The third party had attended Crown Melbourne on three occasions between 2016 and 2017 under Customer 6's junket, turned over $1,540,000,000 and suffered losses of $36,590,000: SMR dated 28 January 2021. As at January 2021, Crown Melbourne still held the HKD26,500,000 as it had been unsuccessful in contacting Customer 6 to return the funds.

On 17 October 2018, a key player under Customer 6's junket, Person 57, decided to stop playing under the junket and play under his own programs. In doing so, the following transactions occurred:

- on 17 October 2018, Person 57 presented $660,000 in cash, sealed in clear plastic bags of $100 and $50 notes, which was counted by a Crown staff member and another individual; and
- once counted, $300,000 was deposited into Person 57's DAB account. The other individual retained the remaining $360,000: SMR dated 18 October 2018.

Unusual transactions and patterns of transactions in 2019

On 19 February 2019, a telegraphic transfer of $364,592 was received into the DAB account of a Crown patron from another Australian casino. Once received, Crown Melbourne was instructed to transfer the funds from the patron's account to Customer 6's Crown Melbourne DAB account, despite the patron not being a key player under any of Customer 6's junket programs at the time: SMR dated 20 February 2019.

On 2 October 2019, a telegraphic transfer of $2,062,698 was sent from Customer 6's Crown Melbourne DAB account to a third party based in Australia: SMR dated 3 October 2019.

Also on 2 October 2019, Customer 6 arranged for a telegraphic transfer of $337,311 from his Crown Perth DAB account to the Australian bank account of the above third party: SMR dated 15 October 2019.

On 16 December 2019, Customer 6's junket representative requested to withdraw $100,000 in cash from Customer 6's DAB account. The cash was to be provided to a key player, who did not have rated wins to support the transactions: SMR dated 18 December 2019.

Unusual transactions in 2020

By January 2021, Customer 6 owed $1,680,265 to Crown Melbourne.

906. On and from November 2016, enquiries by law enforcement agencies relating to Customer 6 raised red flags reflective of higher ML/TF risks for the provision of designated services to Customer 6 at Crown Melbourne and Crown Perth.

Particulars

On 16 November 2016, an enquiry was made by law enforcement in relation to Customer 6.

See particulars to paragraph 902.

907. At no time did Crown Melbourne or Crown Perth undertake appropriate risk-based customer due diligence with respect to Customer 6 with a view to identifying, mitigating and managing the ML/TF risks posed by the provision of designated services on and from 1 March 2016.

a. At no time did Crown Melbourne or Crown Perth take appropriate steps to identify or analyse the ML/TF risks of Customer 6's transactions.

b. At no time did Crown Melbourne or Crown Perth take appropriate steps to identify or analyse the ML/TF risks of Customer 6's transactions or to consider whether they had a lawful purpose.

c. Crown Melbourne or Crown Perth gave no consideration at any time to whether large and high risk transactions should be processed.

d. At no time did Crown Melbourne take appropriate steps to understand whether Customer 6's source of wealth/funds was legitimate, despite Crown Melbourne's knowledge of his connection to the Neptune junket and other UBOs Person 3 and Person 55.

e. On each occasion prior to January 2021 that senior management considered whether to continue the business relationship with Customer 6, senior management failed to give adequate consideration to whether the ML/TF risks posed by Customer 6 were within Crown Melbourne or Crown Perth's risk appetite.

Particulars

Section 36(1)(a) of the Act.

The due diligence steps taken with respect to Customer 6 included:

Database searches

Over the course of 2016, Crown performed risk intelligence searches and company searches on Customer 6.

On 28 October 2016 and 14 August 2017, Crown obtained a risk intelligence report on Customer 6, which identified that Customer 6 was a possible PEP by association and noted that one of Customer 6's companies was identified in an open source offshore companies database.

In 2018, Crown performed further risk intelligence searches, and criminal record checks.

In October 2019, Crown obtained a risk intelligence report on Customer 6 which differed from the 2016 risk intelligence report, in stating that Customer 6 was not a foreign PEP.

Wealth reports

On 24 May 2016 and 17 August 2016, Crown obtained wealth reports on Customer 6 which referred to his alleged detention in 2012 for alleged underground banking and money laundering. Following the receipt of the August 2016 report, Crown Melbourne raised Customer 6's risk rating to significant.

In January 2018, Crown obtained updated wealth reports.

Junket profile

In late 2016 and early 2017, the Credit control team prepared a junket profile on Customer 6 using information obtained from searches and wealth reports, which noted that Customer 6 was detained in 2012 for alleged underground banking and money laundering.

Customer 6's junket profile was updated with details of database searches and wealth information outlined above on 2 October 2017, 26 March 2018, 16 August 2019, and 23 June 2020. Each profile recommended that Crown continue to conduct business, but did not provide a basis for this recommendation.

Senior management consideration

On 4 January 2017, the VIP Operations Committee meeting attended by Chief Executive Officer (Crown Resorts), Executive General Manager (Legal & Regulatory Services), a Crown Resorts director, Chief Executive Officer (Australian Resorts), Senior Vice President

(International Business) and Group General Manager (International Business Operations) considered Customer 6's junket profile. The minutes indicate the Committee requested further information about Customer 6's activities at Crown Aspinalls and deferred further discussion to the following meeting.

In late 2020, Customer 6 was identified by the ILGA inquiry as a junket operator of concern. By 20 November 2020, Crown Melbourne and Crown Perth decided to terminate its relationship with Customer 6.

On 20 November 2020, Crown Melbourne issued an indefinite WOL in respect of Customer 6, and Crown Perth issued an NRL in respect of Customer 6.

Prior to November 2020, none of these steps were proportionate to the ML/TF risks reasonably posed by Customer 6.

On 20 January 2021, the Crown Resorts POI Committee considered Customer 6, who had come to the Committee's attention through the ILGA inquiry. The Committee noted that a WOL and NRL had already been issued in respect of Customer 6 since 20 November 2020.

Following the meeting, Crown Melbourne and Crown Perth increased Customer 6's risk rating to High.

Enhanced customer due diligence

908. Having formed a suspicion for the purposes of s41 of the Act, on and from 1 March 2016, Crown Melbourne gave the AUSTRAC CEO SMRs with respect to Customer 6 on 24 occasions set out in Schedule 3.6.

Particulars

The SMRs reported:

- patterns of suspicions relating to key player win/loss ratios;
- unusual activity by a junket representative of Customer 6's junket;
- transactions with unrelated third parties; and
- transactions indicative of ML/TF typologies.

909. On each occasion that Crown Melbourne formed a suspicion with respect to Customer 6 for the purposes of s41 of the Act, it was required to apply its ECDD program to Customer 6.

Particulars

Rule 15.9(3) of the Rules.

910. Crown Melbourne did not carry out appropriate risk-based ECDD measures with respect to Customer 6 on each occasion that Crown Melbourne formed a suspicion with respect to Customer 6 for the purposes of s41 of the Act.

a. There are no records of ECDD being conducted after giving the AUSTRAC CEO SMRs on 2 March 2016, 23 May 2016, 29 June 2016, 8 July 2016, 5 September 2016, 6 February 2017, 11 July 2017, 17 October 2017, 2 November 2017, 13 November 2017,

14 November 2017, 15 November 2017, 27 December 2017, 2 January 2018, 8 February 2018, 20 February 2018, 27 February 2018, 23 March 2018, 16 April 2018, 17 July 2018, 18 October 2018, 20 February 2019, 3 October 2019, 17 December 2019, and 28 February 2020: see paragraphs 664 and 685.

b. The SMR dated 28 January 2021 was given to the AUSTRAC CEO after Customer 6 was issued with a WOL on 20 November 2020. The SMR identified suspicious conduct on 2 March 2018.

c. Appropriate risk-based steps were not taken to obtain or analyse Customer 6's source of wealth/funds including as a result of his connection to the Neptune junket, Person 3 and Person 55: see paragraph 667.

d. Appropriate risk-based steps were not taken to analyse and monitor Customer 6's transactions – both past and future – including to understand their economic purpose: see paragraphs 590 and 666.

e. On each occasion prior to November 2020 that senior management considered whether to continue the business relationship with Customer 6, senior management failed to give adequate consideration to whether the ML/TF risks posed by Customer 6 were within Crown Melbourne's risk appetite: see paragraph 668ff.

Particulars

Rule 15.9(3), 15.10(1)(c), (d), (2), (5) and (6) of the Rules.

See particulars to paragraph 907.

911. Having formed a suspicion for the purposes of s41 of the Act, on and from 1 March 2016, Crown Perth gave the AUSTRAC CEO SMRs with respect to Customer 6 on 6 February 2018.

Particulars

The SMR dated 6 February 2018 reported on a transfer of $4,000,000 from Customer 6's Crown Perth DAB account to the Crown Melbourne DAB account of another junket operator, Customer 1.

912. On each occasion that Crown Perth formed a suspicion with respect to Customer 6 for the purposes of s41 of the Act, it was required to apply its ECDD program to Customer 6.

Particulars

Rule 15.9(3) of the Rules.

913. Crown Perth did not carry out appropriate risk-based ECDD measures with respect to Customer 6 on each occasion that Crown Perth formed a suspicion with respect to Customer 6 for the purposes of s41 of the Act.

a. There are no records of ECDD being conducted after giving the AUSTRAC CEO an SMR on 6 February 2018: see paragraphs 664 and 685.

b. Appropriate risk-based steps were not taken to obtain or analyse information about Customer 7's source of wealth/funds including as a result of his connection to the Neptune junket, Person 3 and Person 55: see paragraph 667.

c. Appropriate risk-based steps were not taken to analyse and monitor Customer 6's transactions – both past and future – including to understand their economic purpose: see paragraphs 590 and 666.

d. On each occasion prior to November 2020 that senior management considered whether to continue the business relationship with Customer 6, senior management failed to give adequate consideration to whether the ML/TF risks posed by Customer 6 were within Crown Perth's risk appetite: see paragraph 668ff.

Particulars

Rule 15.9(3), 15.10(1)(c), (d), (2), (5) and (6) of the Rules.

See particulars to paragraph 907.

914. By reason of the matters pleaded from paragraphs 888 to 913, on and from 1 March 2016, Crown Melbourne and Crown Perth:

a. did not monitor Customer 6 in relation to the provision of designated services, with a view to identifying, mitigating and managing the ML/TF risks reasonably faced; and

b. did not do so in accordance with rr15.5 and 15.9 of the Rules.

915. By reason of the matters pleaded at paragraph 914, Crown Melbourne and Crown Perth contravened s36(1) of the Act on and from 1 March 2016 to 20 November 2020 with respect to Customer 6.

Particulars

Section 36(1) of the Act is a civil penalty provision: s36(2) of the Act.

Customer 7

916. Customer 7 was a customer of Crown Melbourne from 15 July 2015 to 20 January 2021.

917. From at least 15 July 2015, Crown Melbourne provided Customer 7 with designated services within the meaning of table 1 and table 3, s6 of the Act.

918. From at least 15 July 2015, Customer 7 received designated services as a junket operator for the Neptune junket at Crown Melbourne.

Particulars to paragraphs 917 and 918

On 29 June 2015, Crown Melbourne entered into a NONEGPRA with Customer 7 to operate junkets at Crown Melbourne. Between 2015 and 2016, Customer 7 facilitated at least seven junkets at Crown Melbourne, including one program since 1 March 2016.

On 15 July 2015, Crown Melbourne opened a credit facility (AUD/HKD) in Customer 7's name under his initial and second PIDs. On 30 August 2018, Crown Melbourne closed this credit facility.

On 15 July 2015, Crown Melbourne opened a DAB account and safekeeping account (AUD/HKD) for Customer 7 under the same PIDs.

On 21 September 2015, Crown Melbourne opened a second DAB account and safekeeping account (AUD/HKD) for Customer 7 under a third PID.

On 22 January 2021, Crown Melbourne issued a WOL in respect of Customer 7.

The ML/TF risks posed by Customer 7

919. By 1 March 2016, higher ML/TF risks were indicated by the nature and purpose of Customer 7's business relationship with Crown Melbourne as a junket operator linked to the Neptune junket, his connections to other junket operators and representatives associated with the Neptune junket, including UBOs Person 3 and Person 55, the nature of the transactions he had been conducting, together with the suspicions Crown Melbourne itself had formed with respect to Customer 7.

Particulars

Section 36(1)(a), (b) of the Act and Chapter 15 of the Rules.

Customer 7 was a junket operator. He received designated services through the channel of junket programs. This channel lacked transparency: see paragraph 477.

Links to Neptune junket

From at least 29 June 2015, Crown Melbourne was aware that Customer 7 was connected to the Neptune junket and, as a result, also connected to Person 3, Person 55 and Customer 6 who were the ultimate beneficial owners behind the junket: see paragraph 886.

Junket activity

By 1 March 2016, Customer 7 had operated approximately six junket programs at Crown Melbourne. Crown Melbourne recorded that the total turnover for those programs was $3,510,434,800 with losses of $ 36,999,617. Commissions of $27,251,859 were payable by Crown Melbourne to Customer 7. Crown Melbourne also made a private jet available for use by the Chinatown junket.

By 1 March 2016, Crown management approved numerous credit facilities for Customer 7's junkets prior to the junket programs in various amounts up to AUD$250,000,000 / HKD1,500,000,000, including limits subject to a formal guarantee by other individuals associated with the Neptune junket, Customer 6 and Person 3, who Crown Melbourne understood to be the ultimate beneficial owners of the Neptune junket.

SMRs

By 1 March 2016, Crown Melbourne had given the AUSTRAC CEO seven SMRs in relation to Customer 7. Six SMRs related to losses noted for approximately 28 key players under Customer 7's junket program totalling AUD$50,131,683 and HKD1,347,500 – on 3 August 2015, 1 September 2015, 1 October 2015, 2 November 2015, 7 December 2015, and 7 December 2015.

The remaining SMR related to activities of a key player, Customer 20, under Customer 7's junket on 23 September 2015, involving the exchange of $500,000 in chips for cash by a junket representative on behalf of the key player, in circumstances where the key player already had $1,000,000 in cash in his possession, which was subsequently taken up to his Crown hotel room.

Other red flags

On 15 September 2015, Crown received a law enforcement agency enquiry in relation to transactions on mobiles and suspicious activity at the airport by Customer 7's junket representatives.

In December 2015, the Group General Manager (International Business Operations) approved the transfer of funds of approximately HKD543,000 from Customer 7's Crown Perth DAB account to settle a debt owed by Customer 7 in Crown Melbourne.

Due diligence

By 1 March 2016, the due diligence steps taken with respect to Customer 7 were as follows.

Prior to approving credit for Customer 7 in July 2015, the Credit control team obtained identification documents, risk intelligence searches, company searches and two wealth reports on Customer 7, which detailed Customer 7's position as executive director of a company with links to Person 3 and Person 55.

920. As at 1 March 2016, Customer 7 should have been recognised by Crown Melbourne as a high risk customer for the reasons pleaded at paragraph 919.

Particulars

Section 36(1)(a), (b) of the Act and Chapter 15 of the Rules.

921. At all times on and from 1 March 2016, Customer 7 should have been recognised by Crown Melbourne as a high risk customer by reason of the matters pleaded at paragraphs 919, 923, 925, 926 and 928.

Particulars

Section 36(1)(a), (b) of the Act and Chapter 15 of the Rules.

922. It was not until 20 January 2021 that Crown Melbourne assessed Customer 7 as high risk.

Particulars

On 2 August 2015, 1 September 2015 and 23 March 2018, Crown Melbourne assessed Customer 7 as moderate risk.

On 12 occasions between 11 September 2015 and 1 July 2019, Crown Melbourne assessed Customer 7 as significant risk.

On 21 January 2021, Crown Melbourne assessed Customer 7 as high risk.

See paragraph 481.

923. On and from 1 March 2016, designated services provided to Customer 7 posed higher ML/TF risks including because the provision of designated services to Customer 7 involved a combination of the following factors:

a. Customer 7 was a junket operator for the Neptune junket;

b. at all times, Crown Melbourne was aware of Customer 7's connections to the Neptune junket and its ultimate beneficial owners Person 3, Person 55 and Customer 6. This connection presented high ML/TF risks for the reasons set out at paragraph 886;

c. Customer 7 received high value financial (table 1, s6) and gaming services (table 3, s6) provided through multiple junket programs: see paragraph 473ff;

d. Customer 7 was a junket operator who facilitated the provision of high value financial and gaming services (tables 1 and 3, s6) to key players on his junket programs: see paragraph 473ff;

e. Customer 7 was known at all times to be connected to other junket operators, including junket operators in respect of whom Crown Melbourne or Crown Perth had formed suspicions, such as Customer 6, Customer 8 and Customer 9;

f. designated services provided to Customer 7 lacked transparency as the services were provided through the channel of junket programs: see paragraph 477(e);

g. The table 3, s6 designated services provided to Customer 7 involved high turnover;

h. as at 30 April 2021, Customer 7 had significant parked or dormant funds of $1,307,943 in his safekeeping account at Crown Melbourne, despite the last transaction occurring in the account in January 2016: see paragraph 252;

i. by 16 August 2016, Crown Melbourne was advised that Customer 7 was of interest to the VCGLR;

j. this occurred against the background of:

    i. by 1 March 2016, Crown Melbourne recorded turnover on junket programs operated by Customer 7 that exceeded $3,510,434,800 in just eight months;

    ii. law enforcement having expressed an interest in Customer 7's junket representatives on 15 September 2015;

    iii. seven SMRs being given to the AUSTRAC CEO by 1 March 2016, covering matters including suspicious losses by key players on Customer 7's junket programs and transactions indicative of the ML/TF typology of cashing-in large value chips with no evidence of play; and

    iv. from July 2015, Customer 7 was provided with a significant amount of credit upon request, up to limits of AUD$250,000,000 / HKD1,500,000,000, subject to a guarantee by other junket operators associated with the Neptune junket (Person 3 and Customer 6); and

k. by reason of the matters pleaded at subparagraphs a. to j., and in light of his connections to the Neptune junket, there were real risks that Customer 7's source of wealth/funds were not legitimate.

Monitoring of Customer 7's transactions

924. At no time did Crown Melbourne appropriately monitor Customer 7's transactions on a risk-basis.

Particulars

Section 36(1)(a), (b) of the Act and rules 15.4 to 15.8 of the Rules..

Crown Melbourne was unable to monitor the ML/TF risks posed by the transactions associated with Customer 7's junkets appropriately, including transactions by his junket representatives and key players on his junkets, because it did not make and keep appropriate records of designated services provided: see paragraphs 483ff.

Crown Melbourne did not apply appropriate risk-based transaction monitoring to designated services provided to Customer 7: see paragraphs 590ff and 629 to 642 (designated services) and 643 to 649 (transactions facilitated through junkets).

Ongoing customer due diligence

925. On and from 1 March 2016, on multiple occasions, the provision of designated services to Customer 7 at Crown Melbourne raised red flags reflective of higher ML/TF risks as a result of Customer 7's connections to the Neptune junket and its ultimate beneficial owners Person 3, Person 55 and Customer 6.

Particulars

Section 36(1)(a), (b) of the Act and Chapter 15 of the Rules.

By 1 March 2016, Crown Melbourne and Crown Perth were aware that Person 3, Person 55 and Customer 6 were the ultimate beneficial owners and controllers behind the Neptune junket operators at Crown, including through Customer 9, and had financial interests in the business of the Neptune junket: see paragraph 886.

926. On and from 1 March 2016, on multiple occasions, the provision of designated services to Customer 7 raised red flags reflective of higher ML/TF risks.

Particulars

2016

On 17 August 2016, Crown Melbourne received a VCGLR request for records in relation to junkets and players, including Customer 7. Following this, on 18 August 2016 Crown Melbourne rated Customer 7 as significant risk in connection with this enquiry.

By the end of 2016, Crown Melbourne recorded that Customer 7 was provided with designated services at Crown Melbourne on 40 days during 2016. Crown Melbourne recorded Customer 7's buy-in for 2016 as $5,000 but recorded 'CompExp' as $32,010.

2019

As at 19 January 2022, Customer 7 had a balance of $1,307,943.20 in his DAB account. The account had not been transacted on since January 2016: SMR dated 1 July 2019.

February 2021 – Bergin Report

The Bergin Report found that the Neptune junket had operated junkets within Crown since at least 2005 through a network of various individuals. Notwithstanding adverse media reports that the Neptune junket and its associates were linked to organised crime, Crown continued to allow the junket to operate junket programs at Crown facilities through various other individuals, including Customer 7, but had conceded to the inquiry that the information would be enough to disqualify these operators "going forward".

927. At no time did Crown Melbourne undertake appropriate risk-based customer due diligence with respect to Customer 7 with a view to identifying, mitigating and managing the ML/TF risks posed by the provision of designated services on and from 1 March 2016.

a. At no time did Crown Melbourne take appropriate steps to identify or analyse the ML/TF risks of Customer 7's transactions.

b. At no time did Crown Melbourne take appropriate steps to identify or analyse the ML/TF risks of Customer 7's transactions or to consider whether they had a lawful purpose.

c. Crown Melbourne gave no consideration at any time to whether large and high risk transactions should be processed.

d. At no time did Crown Melbourne take appropriate steps to understand whether Customer 7's source of wealth/funds was legitimate, despite Crown Melbourne's knowledge of his connection to the Neptune junket and ultimate beneficial owners Person 3 and Person 55.

e. On each occasion prior to January 2021 that senior management considered whether to continue the business relationship with Customer 7, senior management failed to give adequate consideration to whether the ML/TF risks posed by Customer 7 was within Crown Melbourne's risk appetite.

Particulars

Section 36(1)(a) of the Act.

The due diligence steps taken with respect to Customer 7 included:

Database searches

In March 2016, the Credit control team obtained information related to Customer 7 based on open source and risk intelligence searches.

In 2017, the Credit control team obtained media articles related to a company associated with Customer 7.

In July 2019, Crown's Group General Manager – AML performed risk intelligence and media searches in respect of Customer 7.

Customer profile

On 23 July 2019, Crown Resorts was asked by a media outlet whether it was aware of open source material allegedly linking the Neptune junket to organised crime.

In response, Crown Melbourne prepared a Patron Information document on Customer 7, which set out key details including risk rating (significant), any law enforcement enquiries, adverse entries in due diligence searches, and gaming activity, which was provided to the Chief Legal Officer.

The document was updated on 17 January 2020 with adverse entries in wealth reports obtained in 2015 and details of the law enforcement enquiries. The document noted that in relation to the alleged connection between the Neptune junket and Person 55, Customer 7 had claimed he was not familiar with Person 55.

Senior management consideration

On 28 March 2018, Crown Melbourne reviewed Customer 7's risk rating and reduced it to moderate.

On 6 December 2018, Crown Melbourne's Group General Manager – AML identified that Customer 7 had $1,300,000 in a DAB account, with no play since 2016, and that he was not presently operating any junkets. No further action was taken.

On 20 January 2021, the Crown Resorts POI Committee considered Customer 7, who had come to the Committee's attention through the ILGA inquiry. The POI Committee issued a WOL against Customer 7, which was applied by Crown Melbourne on 22 January 2021.

Prior to January 2021, none of these steps were proportionate to the ML/TF risks reasonably posed by Customer 7 from 1 March 2016.

Enhanced customer due diligence

928. Having formed a suspicion for the purposes of s41 of the Act, Crown Melbourne gave the AUSTRAC CEO an SMR with respect to Customer 7 on 1 July 2019.

Particulars

The SMR reported parked funds in Customer 7's Crown Melbourne safekeeping account.

929. On each occasion that Crown Melbourne formed a suspicion with respect to Customer 7 for the purposes of s41 of the Act, it was required to apply its ECDD program to Customer 7.

Particulars

Rule 15.9(3) of the Rules.

930. Crown Melbourne did not carry out appropriate risk-based ECDD measures with respect to Customer 7 on each occasion that Crown Melbourne formed a suspicion with respect to Customer 7 for the purposes of s41 of the Act.

a. There are no records of ECDD being conducted after giving the AUSTRAC CEO an SMR dated 1 July 2019: see paragraphs 664 and 685.

b. Appropriate risk-based steps were not taken to obtain or analyse information about Customer 7's source of wealth/funds including as a result of his connection to the Neptune junket and Person 3, Person 55 and Customer 6: see paragraph 667.

c. Appropriate risk-based steps were not taken to analyse and monitor Customer 7's transactions – both past and future – including to understand their economic purpose: see paragraphs 590 and 666.

d. On each occasion prior to January 2021 that senior management considered whether to continue the business relationship with Customer 7, senior management failed to give adequate consideration to whether the ML/TF risks posed by Customer 7 was within Crown Melbourne's risk appetite: see paragraph 668ff.

Particulars

Rule 15.9(3), 15.10(1)(c), (d), (2), (5) and (6) of the Rules.

See particulars to paragraph 927.

931. By reason of the matters pleaded from paragraphs 916 to 930, on and from 1 March 2016, Crown Melbourne:

a. did not monitor Customer 7 in relation to the provision of designated services, with a view to identifying, mitigating and managing the ML/TF risks reasonably faced; and

b. did not do so in accordance with rr15.5 and 15.9 of the Rules.

932. By reason of the matters pleaded at paragraph 931, Crown Melbourne contravened s36(1) of the Act on and from 1 March 2021 to 2022 January 2021 with respect to Customer 7.

Particulars

Section 36(1) of the Act is a civil penalty provision: s36(2) of the Act.

Customer 8

933. Customer 8 was a customer of Crown Melbourne from at least 9 September 2007 to 22 January 2021.

934. From at least 9 September 2007, Crown Melbourne provided Customer 8 with designated services within the meaning of table 1 and table 3, s6 of the Act.

935. From at least 9 September 2007, Customer 8 received designated services as a junket operator for the Neptune junket, as a junket representative for the Neptune junket, and as a junket player facilitated through one junket operator.

Particulars to paragraphs 934 and 935

On 9 September 2007, Crown Melbourne opened a DAB account and safekeeping account (AUD/HKD) for Customer 8 under a first and second PID.

On 18 September 2010, Crown Melbourne opened a credit facility for Customer 8 under an initial and second PID. On 18 September 2010, Crown Melbourne closed this credit facility.

On 6 October 2010, Crown Melbourne entered into a NONEGPRA with Customer 8 to operate junkets at Crown Melbourne.

On 5 August 2019, Customer 8 signed an updated NONEGPRA with both Crown Melbourne and Crown Perth.

Between 2010 and 2016, Customer 8 operated at least 32 junket programs at Crown Melbourne.

Between 17 July 2016 and 3 December 2016, Customer 8 operated two junket programs at Crown Melbourne. During this period, Customer 8 had one junket representative.

Customer 8 received designated services as a junket player through the Customer 7 junket.

Customer 8 was a junket representative for Person 3, Customer 7 and a third junket operator.

On 22 January 2021, Crown Melbourne issued a WOL in respect of Customer 8.

The ML/TF risks posed by Customer 8

936. By 1 March 2016, higher ML/TF risks were indicated by the nature and purpose of Customer 8's business relationship with Crown Melbourne as a junket operator linked to the Neptune junket, his connections to other junket operators and representatives associated with the Neptune junket, including ultimate beneficial owners Person 3 and Person 55, the nature of the transactions he had been conducting, together with the suspicions Crown Melbourne itself had formed with respect to Customer 8.

Particulars

Section 36(1)(a), (b) of the Act and Chapter 15 of the Rules.

Customer 8 was a junket operator, junket representative and junket player. He received designated services through the channel of junket programs. This channel lacked transparency: see paragraph 477.

Links to Neptune junket

From at least 18 September 2010, Crown Melbourne was aware that Customer 8 was connected to the Neptune junket, and, as a result, also connected to Person 3, Person 55 and Customer 6 who were the ultimate beneficial owners behind the junket see paragraph 886.

Crown Melbourne understood that Customer 8 was a "proxy" for Person 55, a principal of the Neptune junket.

Junket activity

By 1 March 2016, Customer 8 had operated approximately 24 junket programs at Crown Melbourne. Crown Melbourne recorded that the

total turnover for those programs was $1,159,923,936, with losses of $19,543,694. Commissions of $9,253,670 were payable by Crown Melbourne to Customer 8.

By 1 March 2016, Crown management approved numerous credit facilities for Customer 8's junkets prior to the junket programs in various amounts in both AUD and HKD ranging from AUD$500,000 to AUD$75,000,000 or HKD1,000,000,000. Crown management also approved a standing credit line with a limit of AUD$5,000,000 between mid-2013 and at least January 2016.

SMRs

By 1 March 2016, Crown Melbourne had given the AUSTRAC CEO five SMRs in relation to Customer 8. Four SMRs related to suspicious telegraphic transfers from Customer 8's Crown Melbourne DAB account, including to unrelated third parties, as follows:

- on 2 June 2008, a third party sent a telegraphic transfer of $330,000 to Customer 8's DAB account when he was acting as a junket representative for Person 3, which was then transferred to Person 3's DAB account: SMR dated 3 June 2008;
- on 28 October 2011, two telegraphic transfers were made from Customer 8's Crown Melbourne DAB account to two third parties of $71,959 to one third party and $1,400,000 to the second third party;
- on 13 January 2012, a telegraphic transfer of HKD1,861,300 (AUD$231,904) was deposited into Customer 8's Crown Melbourne DAB account from a third party; and
- on 1 March 2012, a telegraphic transfer of HKD49,602,300 (AUD$5,863,226) was deposited into Customer 8's Crown Melbourne DAB account from a third party.

The remaining SMR related to a transfer of $5,000,000 from a third party's DAB account to Customer 8's Crown Melbourne DAB account, despite the third party not being a player on any of Customer 8's junkets.

Other red flags

By 1 March 2016, Customer 8 engaged in other unusual or suspicious transactions including in September 2015, when Customer 8 arranged to transfer $96,044 from his Crown Melbourne DAB account to a fellow Neptune Group junket operator's Crown Melbourne DAB account (Customer 7) to satisfy a debt the operator owed to Crown Melbourne.

Due diligence

By 1 March 2016, the due diligence steps taken with respect to Customer 8 were as follows.

By at least 15 June 2012, Crown obtained a Melco Crown due diligence report, which reported that Customer 8 was a guarantor for an overseas junket operation.

On 11 October 2013, Crown prepared a draft profile on the Neptune junket, which reviewed the Neptune Group associates (Customer 8, Customer 9 and Person 3) including their credit lines at other casinos, associated companies, and activities as part of the Neptune junket. The profile described Customer 8 and Customer 9 as acting in the role of "front man" for two other individuals described as "principal partners" (Person 3 and Person 55). No consideration was given to ML/TF risks of Customer 8 acting in a "front man" role for the Neptune junket partners.

Between 2014 and 2016, Crown performed risk intelligence and company searches and obtained wealth reports that confirmed that Customer 8 and Person 3 were business partners in various companies.

937. As at 1 March 2016, Customer 8 should have been recognised by Crown Melbourne as a high risk customer for the reasons pleaded at paragraph 936.

Particulars

Section 36(1)(a), (b) of the Act and Chapter 15 of the Rules.

938. At all times on and from 1 March 2016, Customer 8 should have been recognised by Crown Melbourne as a high risk customer by reason of the matters pleaded at paragraphs 936, 940, 942, 943 and 945.

Particulars

Section 36(1)(a), (b) of the Act and Chapter 15 of the Rules.

939. It was not until 20 January 2021 that Crown Melbourne assessed Customer 8 as high risk.

Particulars

On 12 occasions between 3 June 2008 and 19 September 2013, Crown Melbourne assessed Customer 8 as moderate risk.

On 13 occasions between 20 September 2013 and 7 July 2020, Crown Melbourne assessed Customer 8 as significant risk.

On 20 January 2021, Crown Melbourne assessed Customer 8 as high risk.

See paragraph 481.

940. On and from 1 March 2016 designated services provided to Customer 8 posed higher ML/TF risks including because the provision of designated services to Customer 8 involved a combination of the following factors:

a. Customer 8 was a junket operator and a junket player for the Neptune junket;

b. at all times, Crown Melbourne was aware of Customer 8's connections to the Neptune junket and its ultimate beneficial owners Person 3, Person 55 and Customer 6. This connection presented high ML/TF risks for the reasons set out at paragraph 886;

c. Customer 8 received high value financial service (table 1, s6) and gaming services (table 3, s6), through multiple junket programs: see paragraph 473ff;

d. Customer 8 was a junket operator who facilitated the provision of high value financial and gaming services (tables 1 and 3, s6) to key players on his junket programs: see paragraph 473ff;

e. Customer 8 was known at all times to be connected to other junket operators, including junket operators in respect of whom Crown Melbourne or Crown Perth had formed suspicions such as Customer 7, Customer 9 and Customer 6;

f. designated services provided to Customer 8 lacked transparency as the services were provided through the channel of junket programs: see paragraph 477(e);

g. the table 3, s6, designated services provided to Customer 8 involved high turnover;

h. designated services provided to Customer 8 involved large transfers to and from third parties, including to and from other junket operators and unknown third parties: see paragraph 456ff;

i. designated services provided to Customer 8 involved large cross-border movements of funds: see paragraph 238(d);

j. large values were transferred to and from Customer 8's DAB account and other customers' DAB accounts, involving the provision by Crown Melbourne of designated services within the meaning of items 31 and 32, table 1, s6 of the Act: see paragraphs 411ff and 492;

k. these transactions took place against the background of:

   i. by 1 March 2016, Crown Melbourne had recorded that turnover on junket programs operated by Customer 8 had exceeded $1,159,923,936;

   ii. five SMRs being given to the AUSTRAC CEO by 1 March 2016, covering matters including unusual transfers to other junket operators (Person 3 and Customer 7) and third parties;

   iii. by 1 March 2016, Customer 8 was provided with significant amounts of credit upon request, up to limits of AUD$75,000,000 or HKD1,000,000,000, including a standing credit line with a limit of $5,000,000 which was reapproved on a regular basis from mid-2013: see paragraphs 280ff and 487; and

l. by reason of the matters pleaded at subparagraphs a. to k, and in light of his connections to the Neptune junket, there were real risks that Customer 8's source of wealth/funds were not legitimate.

Monitoring of Customer 8's transactions

941. At no time did Crown Melbourne appropriately monitor Customer 8's transactions on a risk-basis.

Particulars

Section 36(1)(a), (b) of the Act and rules 15.4 to 15.8 of the Rules..

Crown Melbourne was unable to monitor the ML/TF risks posed by Customer 8's transactions appropriately because it did not make and

keep appropriate records of designated services provided to junket players: see paragraphs 483ff.

Crown Melbourne did not apply appropriate risk-based transaction monitoring to designated services provided to Customer 8: see paragraphs 590ff and 629 to 642 (designated services) and 643 to 649 (transactions facilitated through junkets).

Ongoing customer due diligence

942. On and from 1 March 2016, on multiple occasions, the provision of designated services to Customer 8 at Crown Melbourne raised red flags reflective of higher ML/TF risks as a result of Customer 8's connections to the Neptune junket and its ultimate beneficial owners Person 3, Person 55 and Customer 6.

Particulars

Section 36(1)(a), (b) of the Act and Chapter 15 of the Rules.

By 1 March 2016, Crown Melbourne and Crown Perth were aware that Person 3, Person 55 and Customer 6 were the ultimate beneficial owners and controllers behind the Neptune junket operators at Crown, including through Customer 8, and had financial interests in the business of the Neptune junket: see paragraph 886.

943. On and from 1 March 2016, on multiple occasions, the provision of designated services to Customer 8 raised red flags reflective of higher ML/TF risks.

Particulars

2016

Between 3 March 2016 and 17 November 2016, Crown management regularly approved Customer 8's standing credit line to a limit of $5,000,000, although no junket programs were operated during this period.

On 18 November 2016, Customer 8 operated a junket program at Crown Melbourne. Crown Melbourne recorded that the junket's buy-in for that trip was $5,000,000 with losses of $3,439,805. Commissions of $384,000 were payable by Crown Melbourne to Customer 8.

On 3 December 2016, Customer 8 operated a junket program at Crown Melbourne. The junket's buy-in was $5,000,000 with turnover of $24,000,000. Commissions of $336,000 were payable by Crown Melbourne to Customer 8.

By 5 December 2016, Crown Melbourne was aware of high losses noted for key players on Customer 8's junket, totalling $3,469,750 for one player.

On 19 December 2016, a telegraphic transfer of $3,056,000 was deposited into Customer 8's Crown Melbourne DAB account from a third party based overseas: SMR dated 20 December 2016.

2018

In February 2018, Customer 8 submitted a request to reactivate his credit line at Crown Melbourne to $30,000,000 which was approved by Crown management on 15 February 2018, however no junket programs were operated.

2019

By March 2019, Customer 8 had not attended or run a junket program at Crown Melbourne since December 2016. However, the following transactions were processed by Crown Melbourne through his DAB account:

- on 26 March 2019, a third party transferred $292,918 from another Australian casino into Customer 8's DAB account. Following this, Crown Melbourne processed a transfer of $300,000 from Customer 8's Crown Melbourne DAB account to a third party's DAB account: SMR dated 27 March 2019. The third party had not previously been associated with Customer 8's junkets and had suffered losses on other junket programs at Crown in 2019 as well as on individual rated gaming activity; and
- on 29 March 2019, Crown Melbourne arranged a telegraphic transfer of $206,449 from the third party's DAB account to another third party based overseas: SMR dated 1 April 2019.

February 2021 – Bergin Report

The Bergin Report found that the Neptune junket had operated junkets within Crown since at least 2005 through a network of various individuals. Notwithstanding adverse media reports that the Neptune junket and its associates were linked to organised crime, Crown continued to allow the junket to operate junket programs at Crown facilities through various other individuals, including Customer 8, but had conceded to the inquiry that the information would be enough to disqualify these operators "going forward".

944. At no time did Crown Melbourne undertake appropriate risk-based customer due diligence with respect to Customer 8 with a view to identifying, mitigating and managing the ML/TF risks posed by the provision of designated services on and from 1 March 2016.

a. At no time did Crown Melbourne take appropriate steps to identify or analyse the ML/TF risks of Customer 8's transactions.

b. At no time did Crown Melbourne take appropriate steps to identify or analyse the ML/TF risks of Customer 8's transactions or to consider whether they had a lawful purpose.

c. Crown Melbourne gave no consideration at any time to whether large and high risk transactions should be processed.

d. At no time did Crown Melbourne take appropriate steps to understand whether Customer 8's source of wealth/funds was legitimate, despite Crown Melbourne's knowledge of his connection to the Neptune junket, Person 3 and Person 55.

e. On each occasion prior to January 2021 that senior management considered whether to continue the business relationship with Customer 8, senior management failed to give adequate consideration to whether the ML/TF risks posed by Customer 8 was within Crown Melbourne's risk appetite.

Particulars

Section 36(1)(a) of the Act.

The due diligence steps taken with respect to Customer 8 included:

Database searches

Between February 2016 and May 2016, the Credit control team performed open source, risk intelligence, company and property title searches for companies linked to Customer 8.

In February 2020, Crown Melbourne performed a search of its surveillance database, which returned no records related to Customer 8, but noted that numerous SMRs had been given to the AUSTRAC CEO in relation to Customer 8.

Wealth reports

Between February 2016 and May 2016, Crown obtained wealth reports on Customer 8, which indicated that Customer 8 was a shareholder of companies connected to the Neptune junket. Additional wealth reports were obtained in 2018 and 2020.

Junket profile

By 2 March 2017, the Credit control team prepared a junket profile on Customer 8. The junket profile incorporated searches and information obtained in 2016 and 2017 and noted that Customer 8 was linked to Person 3 and Person 55. It also summarised media articles dated 2012 and 2015 articles which indicated that Person 55 had been charged with money laundering.

On 14 February 2018 and 18 February 2020, the Credit control team updated Customer 8's junket profile. Each iteration recommended that Crown continue to do business with Customer 8.

Senior management consideration

On 2 March 2017, the VIP Operations Committee attended by the Senior Vice President (International Business), CEO (Australian Resorts), Group General Manager (International Business Operations), a Crown Resorts director, Group General Counsel (Crown Resorts), Executive General Manager (Legal & Regulatory Services) considered Customer 8's junket profile. The minutes noted that Customer 8's business partner, Person 3, had been charged with money laundering. Despite this, it appears that the attendees recommended that Crown continue to conduct business with Customer 8.

On 20 January 2021, the Crown Resorts POI Committee considered Customer 8, who had come to the Committee's attention through the ILGA inquiry. The POI committee issued a WOL in respect of Customer 8, which took effect on 22 January 2021.

Prior to January 2021, none of these steps were proportionate to the ML/TF risks reasonably posed by Customer 8 from 1 March 2016.

Enhanced customer due diligence

945. Having formed a suspicion for the purposes of s41 of the Act, Crown Melbourne gave the AUSTRAC CEO SMRs with respect to Customer 8 on:

a. 5 December 2016;

b. 20 December 2016;

c. 27 March 2019; and

d. 1 April 2019.

Particulars

Each of these SMRs reported suspicious telegraphic transfers from third parties or suspicious losses noted for key players on Customer 8's junkets.

946. On each occasion that Crown Melbourne formed a suspicion with respect to Customer 8 for the purposes of s41 of the Act, it was required to apply its ECDD program to Customer 8.

Particulars

Rule 15.9(3) of the Rules.

947. Crown Melbourne did not carry out appropriate risk-based ECDD measures with respect to Customer 8 on each occasion that Crown Melbourne formed a suspicion with respect to Customer 8 for the purposes of s41 of the Act.

a. There are no records of ECDD being conducted after giving the AUSTRAC CEO SMRs on 20 December 2016, 27 March 2019 and 1 April 2019: see paragraphs 664 and 685.

b. Appropriate risk-based steps were not taken to obtain or analyse information about Customer 8's source of wealth/funds, including as a result of his connection to the Neptune junket and Person 3, Person 55 and Customer 6: see paragraph 667.

c. Appropriate risk-based steps were not taken to analyse and monitor Customer 8's transactions – both past and future – including to understand their economic purpose: see paragraphs 590 and 666.

d. On each occasion prior to January 2021 that senior management considered whether to continue the business relationship with Customer 8, senior management failed to give adequate consideration to whether the ML/TF risks posed by Customer 8 was within Crown Melbourne's risk appetite: see paragraph 668ff.

Particulars

Rule 15.9(3), 15.10(1)(c), (d), (2), (5) and (6) of the Rules.

See particulars to paragraph 944.

948. By reason of the matters pleaded at paragraphs 933 to 947, on and from 1 March 2016, Crown Melbourne:

a. did not monitor Customer 8 in relation to the provision of designated services, with a view to identifying, mitigating and managing the ML/TF risks reasonably faced; and

b. did not do so in accordance with rr15.5 and 15.9 of the Rules.

949. By reason of the matters pleaded at paragraph 948, Crown Melbourne contravened s36(1) of the Act on and from 1 March 2016 to 22 January 2021 with respect to Customer 8.

Particulars

Section 36(1) of the Act is a civil penalty provision: s36(2) of the Act.

Customer 9

950. Customer 9 was a customer of Crown Melbourne between 8 June 2011 and 22 January 2021.

951. From at least 8 June 2011, Crown Melbourne provided Customer 9 with designated services within the meaning of table 1 and table 3, s6 of the Act.

952. From at least 8 June 2011 to 25 February 2020, Customer 9 received designated services as a junket operator for the Neptune junket and as an independent junket operator, as a junket representative for the Neptune junket and as a junket player at Crown Melbourne.

Particulars to paragraphs 951 and 952

On 30 May 2011, Crown Melbourne entered into a NONEGPRA with Customer 9 to operate junkets at Crown Melbourne.

On 8 June 2011, Crown Melbourne opened a credit facility (AUD/HKD) in Customer 9's name under an initial and second PIDs. On 19 May 2020, Crown Melbourne closed this credit facility.

On 21 July 2011, Crown Melbourne opened a DAB account and safekeeping account (AUD/HKD) for Customer 9 under the same PIDs.

On 10 August 2014, Crown Melbourne opened a second DAB account and safekeeping account (AUD/HKD) for Customer 9 under a third and fourth PID.

On 24 November 2019, Crown Melbourne opened two further DAB account and safekeeping accounts for Customer 9 under a fifth and sixth PID.

Between 2011 and 2020, Customer 9 facilitated at least 31 junkets at Crown Melbourne. Between 2 September 2016 and 26 February 2020, Customer 9 operated at least four junkets at Crown Melbourne under his first PID.

Customer 9 was a junket representative for Person 3.

Customer 9 received designated services through his own junket and Customer 7's junket, which was also part of the Neptune junket.

The ML/TF risks posed by Customer 9

953. By 1 March 2016, higher ML/TF risks were indicated by the nature and purpose of Customer 9's business relationship with Crown Melbourne as a junket operator linked to the Neptune junket, his connections to other junket operators and representatives associated with the Neptune junket, including ultimate beneficial owners Person 3 and Person 55, the nature of the transactions he had been conducting, together with the suspicions Crown Melbourne itself had formed with respect to Customer 9.

Particulars

Section 36(1)(a), (b) of the Act and Chapter 15 of the Rules.

Customer 9 was a junket operator. He received designated services through the channel of junket programs. This channel lacked transparency: see paragraph 477.

Links to Neptune junket

From at least 30 May 2011, Crown Melbourne was aware that Customer 9 was connected to the Neptune junket and, as a result, also connected to Person 3, Person 55 and Customer 6 who were the ultimate beneficial owners behind the junket: see paragraph 886.

Junket activity

By 1 March 2016, Customer 9 had operated at least 27 junket programs at Crown Melbourne. The total turnover for those programs was $818,104,727 with losses of $9,400,967. Between 2011 and 2014, Crown Melbourne paid at least $1,148,213 in commissions to Customer 9.

By 1 March 2016, Crown management approved numerous credit facilities for Customer 9's junkets in various amounts ranging from $500,000 to $14,171,589, including limits subject to an informal guarantee by Person 3 and Person 55, who Crown Melbourne understood to be the ultimate beneficial owners of the Neptune junket.

SMRs

By 1 March 2016, Crown Melbourne had given the AUSTRAC CEO nine SMRs in relation to Customer 9. Two SMRs related to losses noted for the key players under Customer 9's junket program – on 5 November 2012 and 27 November 2015.

Two SMRs related to suspicious transfers between Customer 9's Crown DAB account and other DAB accounts as follows:

- on 29 July 2014, $715,517 was transferred from Customer 9's DAB account to his junket representative's DAB account, then $100,000 was forwarded to a third party: SMR dated 30 July 2014; and
- on 20 August 2014, $10,000,000 was transferred from Customer 6's Crown Melbourne DAB account to Customer 9's Crown Melbourne DAB account: SMR dated 21 August 2014.

Three SMRs related to suspicious telegraphic transfers from Customer 9's Crown Melbourne DAB account, including to unrelated third parties, as follows:

- on 23 August 2011, a telegraphic transfer of $300,000 was sent from Customer 9's Crown Melbourne DAB account to a third party: SMR dated 23 August 2011;
- on 11 October 2011, a telegraphic transfer of $2,102,900 was sent from Person 3's DAB account to Customer 9's overseas bank account: SMR dated 12 October 2011; and
- on 1 August 2014, two telegraphic transfers were sent from Customer 9's Crown Melbourne DAB account to third parties, including $390,000 to a third party based overseas, and $1,750,000 to a third party based in Australia: SMR dated 4 August 2014.

The SMRs reported overseas cash deposits via the City of Dreams deposit service (see paragraphs 332ff and 334ff) and Aspinalls deposit service (see paragraphs 332ff and 375ff) to repay credit markers issued to Customer 9 by Crown Melbourne, as follows:

- on 18 February 2015, HKD64,816,736 was deposited via the City of Dreams overseas deposit service by a third party who was not a key player under any of Customer 9's junket programs: SMR dated 19 February 2015;
- the above transaction was part of a series of transactions facilitated by Crown Melbourne in February 2015, in order to make funds available to Customer 9 for the purposes of repaying a credit marker to Crown Melbourne, including:
    - a remittance of GBP1,542,479 from Customer 9's Crown Aspinalls account to Crown Melbourne; and
    - a telegraphic transfer of AUD$1,078,076 from Customer 9's account at another Australian casino to Crown Melbourne; and
- on 3 November 2015, HKD971,104 was deposited via the City of Dreams deposit service by a third party who was not a key player under any of Customer 9's junket programs, to be credited to Customer 9's Crown DAB account.

Other red flags

In addition to the transactions reported above:

- on 29 January 2014, a third party company deposited $65,452 into Crown Melbourne's Australian bank account for the benefit of Customer 9. Crown Melbourne recognised that the company was not a money changer, nor was Customer 9 linked to the company and requested that the funds be returned;

- on 25 February 2015, Crown Aspinalls confirmed it was holding GBP600,000 for benefit of Customer 9 to purchase gaming chips at Crown Melbourne, and stated that Crown Melbourne was authorised to request remittance of the funds to cover any losses;
- on 5 June 2015, there was a third City of Dreams transaction related to the City of Dreams deposit service, involving a third party who deposited HKD25,408,350 in cash at City of Dreams, on behalf of Customer 9 to repay a credit marker issued by Crown Perth; and
- on 24 December 2015, there was a fourth City of Dreams transaction related to the City of Dreams deposit service Customer 9's "junket assistant" deposited HKD2,578,400 in cash into Customer 9's account at City of Dreams. City of Dreams remitted the funds to Crown Melbourne to repay a credit marker issued to Customer 9 by Crown Melbourne.

Due diligence

By 1 March 2016, the due diligence steps taken with respect to Customer 9 were as follows.

On 11 October 2013, Crown prepared a draft profile on the Neptune Group, which reviewed the Neptune junket associates (Customer 8, Customer 9 and Person 3): see particulars to paragraph 936.

Between 21 October 2013 and 28 October 2013, some due diligence checks were performed on individuals, associated with the Neptune junket, including Customer 9. The checks confirmed that a regulator had queried another Australian casino's association with the Neptune Group during its casino license review. The General Manager – Compliance concluded that Neptune was reported to have links to organised crime but charges were dropped for lack of evidence, and that on this basis there was "nothing definitive" for "AUSTRAC purposes" to prevent Crown from dealing with the Neptune junket.

954. As at 1 March 2016, Customer 9 should have been recognised by Crown Melbourne as a high risk customer for the reasons pleaded at paragraph 953.

Particulars

Section 36(1)(a), (b) of the Act and Chapter 15 of the Rules.

955. At all times on and from 1 March 2016, Customer 9 should have been recognised by Crown Melbourne as a high risk customer by reason of the matters pleaded at paragraphs 953, 957, 958, 959, 960 and 962.

Particulars

Section 36(1)(a), (b) of the Act and Chapter 15 of the Rules.

956. It was not until 20 January 2021 that Crown Melbourne assessed Customer 9 as high risk.

Particulars

On 17 occasions between 23 August 2011 and 30 October 2019, Crown Melbourne assessed Customer 9 as moderate risk.

On 20 January 2021, Crown Melbourne assessed Customer 9 as high risk

See paragraph 481.

957. On and from 1 March 2016 designated services provided to Customer 9 posed higher ML/TF risks including because the provision of designated services to Customer 9 involved a combination of the following factors:

a. Customer 9 was a junket operator for the Neptune junket, a junket representative for the Neptune junket and a junket player (including on the Neptune junket);

b. at all times, Crown Melbourne was aware of Customer 9's connections to the Neptune junket and its ultimate beneficial owners Person 3, Person 55 and Customer 6. This connection presented high ML/TF risks for the reasons set out at paragraph 886;

c. Customer 9 received high value financial (table 1, s6) and gaming services (table 3, s6) provided through multiple junket programs: see paragraph 473ff;

d. Customer 9 was a junket operator who facilitated the provision of high value financial and gaming services (tables 1 and 3, s6) to key players on his junket programs: see paragraph 473ff;

e. Customer 9 was known at all times to be connected to other junket operators, including junket operators in respect of whom Crown Melbourne or Crown Perth had formed suspicions such as Customer 6, Customer 7 and Customer 8;

f. designated services provided to Customer 9 lacked transparency as the services were provided through the channel of junket programs: see paragraph 477(e);

g. designated services provided to Customer 6 lacked transparency because he operated junket programs for both for the Neptune junket and as an independent junket operator;

h. the table 3, s6 designated services provided to Customer 9 involved high turnover;

i. designated services provided to Customer 9 involved large transfers to and from third parties, including to and from other junket operators and unknown third parties: see paragraph 456ff;

j. designated services provided to Customer 9 involved large cross-border movements of funds: see paragraph 238(d);

k. large values were transferred to and from Customer 9's DAB account, and to and from other customers' DAB accounts, involving the provision by Crown Melbourne of designated services within the meaning of items 31 and 32, table 1, s6 of the Act: see paragraphs 411ff and 492;

l. at various times, Customer 9 was provided with significant amounts of credit upon request, up to limits of $20,000,000 in 2018: see paragraphs 280ff and 487;

m. at various times, Customer 9 had significant parked or dormant funds in his DAB account: see paragraph 252;

n. these transactions took place against the background of:

i. by 1 March 2016, Crown Melbourne recorded that turnover on junket programs operated by Customer 9 exceeded $818,104,727;

ii. Crown Melbourne was aware of suspicious transactions involving Customer 6 and Customer 9, in which $10,000,000 was transferred through their Crown Melbourne DAB accounts;

iii. Customer 9 had repaid debts to Crown Melbourne arising from outstanding credit markers by depositing cash through agents at the City of Dreams casino: see paragraphs 332ff and 334ff; and

iv. nine SMRs being given to the AUSTRAC CEO by 1 March 2016; and

o. by reason of the matters pleaded at subparagraphs a. to n., and in light of his connections to the Neptune junket, there were real risks that Customer 9's source of wealth/funds were not legitimate.

Monitoring of Customer 9's transactions

958. At no time did Crown Melbourne appropriately monitor Customer 9's transactions on a risk-basis.

Particulars

Section 36(1)(a), (b) of the Act and rules 15.4 to 15.8 of the Rules..

Crown Melbourne was unable to monitor the ML/TF risks posed by Customer 9's transactions appropriately because it did not make and keep appropriate records of designated services provided to junket operators or players: see paragraphs 483ff.

Crown Melbourne did not apply appropriate risk-based transaction monitoring to designated services provided to Customer 9: see paragraphs 590ff and 629 to 642 (designated services) and 643 to 649 (transactions facilitated through junkets).

Customer 9's transactions involved transactions indicative of ML/TF typologies and vulnerabilities that were not detected prior to a 2021 lookback. Had appropriate risk-based transaction monitoring been applied, these transactions could have been identified earlier: see paragraphs 686 and 687.

In 2021, an independent expert identified transactions as indicative of the ML/TF typology of parking: Customer 9 had parked $93,190 in his safekeeping account at Crown Melbourne, and there had been no activity on the account since 13 March 2020.

Ongoing customer due diligence

959. On and from 1 March 2016, on multiple occasions, the provision of designated services to Customer 9 at Crown Melbourne raised red flags reflective of higher ML/TF risks as a result of Customer 9's connections to the Neptune junket and its ultimate beneficial owners Person 3, Person 55 and Customer 6.

Particulars

Section 36(1)(a), (b) of the Act and Chapter 15 of the Rules.

By 1 March 2016, Crown Melbourne and Crown Perth were aware that Person 3, Person 55 and Customer 6 were the ultimate beneficial owners and controllers behind the Neptune junket operators at Crown, including through Customer 9, and had financial interests in the business of the Neptune junket: see paragraph 886.

February 2021 – Bergin Report

The Bergin Report found that the Neptune junket had operated junkets within Crown since at least 2005 through a network of various individuals. Notwithstanding adverse media reports that the Neptune junket and its associates were linked to organised crime, Crown continued to allow the junket to operate junket programs at Crown facilities through various other individuals, including Customer 9, but had conceded to the inquiry that the information would be enough to disqualify these operators "going forward".

960. On and from 1 March 2016, on multiple occasions, the provision of designated services to Customer 9 raised red flags reflective of higher ML/TF risks arising from Customer 9's junket activity.

Particulars

See paragraph 477.

2016

Between 18 October 2016 and 24 October 2016, Customer 9 was the junket operator of a junket program at Crown Melbourne. Crown Melbourne recorded that the junket's buy-in was $5,000,000 with turnover of $31,270,000 and wins of $4,300,000. A commission of $250,160 was payable by Crown Melbourne to Customer 9.

At settlement, Customer 9 arranged for Crown Melbourne to telegraphic transfer $4,511,793 to one of the key player's overseas bank accounts. However, Crown Melbourne formed suspicions as this amount was inconsistent with the wins noted for the key player under the junket program – the key player was only noted to have won $665,000: SMR dated 7 November 2016.

2017

Around 14 January 2017, Customer 9 was the junket operator of a junket program at Crown Melbourne. Crown Melbourne recorded that the junket's buy-in was $2,510,460 with turnover of $31,270,000 and losses of $2,391,831. A commission of $477,621 was payable by Crown Melbourne to Customer 9.

On 15 August 2017, Crown management approved a credit facility with a limit of HKD20,000,000 for Customer 9 to run a junket program in Crown Melbourne.

2018 to 2019

On 8 March 2018, Crown management agreed to increase Customer 9's credit facility limit from HKD20,000,000 to AUD$20,000,000.

By September 2019, Crown Melbourne recorded that Customer 9 had been "inactive" (i.e. had not facilitated a junket program, despite being approved for credit in March 2018), at Crown Melbourne since January 2017.

By late 2019, Customer 9 sought approval from Crown management to recommence junket operations at Crown Melbourne. Approval was granted by 22 November 2019. Following approval, on 24 November 2019, Crown Melbourne opened two further DAB accounts and safekeeping accounts for Customer 9 under a fifth and sixth PID.

On 10 February 2020, Crown management agreed to approve a credit facility with a limit of AUD$10,000,000 for use by Customer 9's junket program.

2020

Around 21 February 2020, Customer 9 was the junket operator of a junket program at Crown Melbourne. Crown Melbourne recorded that Customer 9's individual turnover as a key player for that trip was HKD78,930,000, with total wins of HKD3,858,000. Crown Melbourne recorded that the total turnover for Customer 9's junket program was HKD263,900,000. Commissions of HKD3,430,700 were payable by Crown Melbourne to Customer 9.

Following the closure of the junket program, Customer 9 left $93,190 in his safekeeping account at Crown Melbourne. The funds were still parked in the account as at 18 June 2021. There has been no activity on the DAB or safekeeping accounts since 13 March 2020.

961. At no time did Crown Melbourne undertake appropriate risk-based customer due diligence with respect to Customer 9 with a view to identifying, mitigating and managing the ML/TF risks posed by the provision of designated services on and from 1 March 2016.

a. At no time did Crown Melbourne take appropriate steps to identify or analyse the ML/TF risks of Customer 9's transactions.

b. At no time did Crown Melbourne take appropriate steps to identify or analyse the ML/TF risks of Customer 9's transactions or to consider whether they had a lawful purpose.

c. With the exception of the attempted deposit of $65,452 from a third party company into Customer 9's DAB account on 29 January 2014, Crown Melbourne gave no consideration at any time to whether large and high risk transactions should be processed.

d. At no time did Crown Melbourne take appropriate steps to understand whether Customer 9's source of wealth/funds was legitimate, despite Crown Melbourne's knowledge of his connection to the Neptune junket, Person 3 and Person 55.

e. On each occasion prior to January 2021 that senior management considered whether to continue the business relationship with Customer 9, senior management failed to give

adequate consideration to whether the ML/TF risks posed by Customer 9 were within Crown Melbourne's risk appetite.

Particulars

Section 36(1)(a) of the Act.

The due diligence steps taken with respect to Customer 9 included:

Database searches

In late 2016, late 2017 and October 2019, the Credit control team performed database searches including risk intelligence, property title and company searches for entities linked to Customer 9.

Prior to Customer 9's attendance at Crown Melbourne in February 2020, Crown Melbourne checked whether Customer 9 was recorded in its surveillance or SEER databases.

Wealth information

In late 2016, the Credit control team obtained wealth reports on Customer 9.

On 31 October 2019, the Credit control team obtained updated wealth reports on Customer 9, which referred to the reputational and jurisdictional risks of doing business with Customer 9.

Junket profiles

In late 2016 and early 2017, the Credit control team prepared a junket profile on Customer 9. In October 2017, 23 March 2018, August 2019, 8 November 2019, and 20 May 2020, the Credit control team updated Customer 9's junket profile, which recommended that Crown continue to do business with Customer 9 but did not provide a basis for this decision.

Senior management consideration

On 5 January 2017, a Crown employee enquired with an overseas Crown employee whether Customer 9 was still affiliated with the Neptune Group, as "a silent partner" or if he operated behind the scenes. The employee also sought information on how Customer 9 operated his junket (whether he sourced his own clients or was referred by another junket operator). On 5 January 2017, the overseas Crown employee confirmed that Customer 9 had a close relationship with the Neptune junket and was also an independent junket operator.

On 12 January 2017, the VIP Operations Meeting attended by the Chief Executive Officer (Crown Resorts), Executive General Manager (Legal and Regulatory Services), Chief Executive Officer (Australian Resorts), Senior Vice President (International Business) and Group General Manager (International Business Operations), considered Customer 9's junket profile, which noted that through his connections to the Neptune junket Customer 9 was deemed to be associated with an individual affiliated with organised crime (Person 55) and another

individual convicted of money laundering. There is no record of any decision taken in relation to the meeting.

On 12 September 2020, Crown obtained a report from an external due diligence provider into a number of subjects including Customer 9, which disclosed that Customer 9 was associated with an individual who had been arrested though not convicted by foreign authorities for illegal gambling, and with Person 3 who had links to money laundering.

On 20 January 2021, the Crown Resorts POI Committee considered Customer 9, who had come to the Committee's attention through the ILGA inquiry, and issued a WOL in respect of Customer 9.

On 22 January 2021, the WOL against Customer 9 took effect at Crown Melbourne.

Prior to January 2021, none of these steps were proportionate to the ML/TF risks reasonably posed by Customer 9 on and from 1 March 2016.

Enhanced customer due diligence

962. Having formed a suspicion for the purposes of s41 of the Act, Crown Melbourne gave the AUSTRAC CEO an SMR with respect to Customer 9 on 7 November 2016.

Particulars

The SMR described a telegraphic transfer of $4,511,793 sent from Customer 9's DAB account to a key player's bank account overseas, in circumstances where the amount of the telegraphic transfer was not consistent with the wins noted for that player.

963. On each occasion that Crown Melbourne formed a suspicion with respect to Customer 9 for the purposes of s41 of the Act, it was required to apply its ECDD program to Customer 9.

Particulars

Rule 15.9(3) of the Rules.

964. Crown Melbourne did not carry out appropriate risk-based ECDD measures with respect to Customer 9 on each occasion that Crown Melbourne formed a suspicion with respect to Customer 9 for the purposes of s41 of the Act.

a. There are no records of ECDD being conducted after giving the AUSTRAC CEO an SMR on 7 November 2016: see paragraphs 664 and 685.

b. Appropriate risk-based steps were not taken to obtain or analyse information about Customer 9's source of wealth/funds, including as a result of his connection to the Neptune junket and Person 3, Person 55 and Customer 6: see paragraph 667.

c. Appropriate risk-based steps were not taken to analyse and monitor Customer 9's transactions – both past and future – including to understand their economic purpose: see paragraphs 590 and 666.

d. On each occasion prior to January 2021 that senior management considered whether to continue the business relationship with Customer 9, senior management failed to give

adequate consideration to whether the ML/TF risks posed by Customer 9 were within Crown Melbourne's risk appetite: see paragraph 668ff.

Particulars

Rule 15.9(3), 15.10(1)(c), (d), (2), (5) and (6) of the Rules.

See particulars to paragraph 961.

965. By reason of the matters pleaded from paragraphs 950 to 964, on and from 1 March 2016, Crown Melbourne:

a. did not monitor Customer 9 in relation to the provision of designated services, with a view to identifying, mitigating and managing the ML/TF risks reasonably faced; and

b. did not do so in accordance with rr15.5 and 15.9 of the Rules.

966. By reason of the matters pleaded at paragraph 965, Crown Melbourne contravened s36(1) of the Act on and from 1 March 2016 to 22 January 2021 with respect to Customer 9.

Particulars

Section 36(1) of the Act is a civil penalty provision: s36(2) of the Act.

CHINATOWN JUNKET

967. At various times between 2014 to December 2019, Crown Melbourne and Crown Perth had a NONEGPRA with junket operators who were part of a network of junket operators affiliated with Person 41 (**Chinatown junket**),.

a. Between 2014 and 2016, the Chinatown junket operated at Crown Melbourne and Crown Perth through a series of junket operators, including Customer 10, Customer 11, Customer 12 and Customer 13.

Particulars

Customer 10

On 24 August 2014, Crown Melbourne and Customer 10 entered into a NONEGPRA. Customer 10 operated junket programs at Crown Melbourne until approximately November 2015.

On 24 September 2014, Crown Perth and Customer 10 entered into a NONEGPRA. Customer 10 operated junket programs at Crown Perth until approximately November 2015.

The Chinatown junket switched its junket operators from Customer 10 to Customer 11 in approximately August 2015.

Customer 11

On 27 August 2015, Crown Melbourne and Customer 11 entered into a NONEGPRA. Customer 11 operated junket programs at Crown Melbourne until approximately April 2016.

On 27 August 2015, Crown Perth and Customer 11 entered into a NONEGPRA. Customer 11 operated junket programs at Crown Perth until approximately March 2016.

The Chinatown junket switched its junket operators from Customer 11 to Customer 12 in approximately April 2016.

Customer 12

On 21 April 2016, Crown Melbourne and Customer 12 entered into a NONEGPRA. Customer 12 operated junket programs at Crown Melbourne until approximately October 2016.

By at least 22 April 2016, Crown Perth and Customer 12 entered into a NONEGPRA. Customer 12 operated junket programs at Crown Perth until approximately July 2016.

The Chinatown junket switched its junket operators from Customer 12 to Customer 13 in approximately September 2016.

Customer 13

On 17 September 2016, Crown Melbourne and Customer 13 entered into a NONEGPRA. Customer 13 operated one junket program at Crown Melbourne in 2016.

b. On and from September 2017 to 2020, Crown Melbourne should have known that the Chinatown junket was continuing operations at Crown Melbourne through a junket operator, Customer 14.

Customer 14

On 6 September 2017, Crown Melbourne and Customer 14 entered into a NONEGPRA. Customer 14 operated junket programs at Crown Melbourne until 2019.

c. Between 2014 and 2019, the junket operators associated with the Chinatown junket were represented by common junket representatives.

Particulars

Common junket representatives included Person 23 and Person 40.

d. Between 2015 and 2016, credit facilities and limits approved for junket operators associated with the Chinatown junket were guaranteed by common third parties.

Particulars

Person 25 guaranteed credit facilities for Customer 11, Customer 12, and Customer 13.

Person 39 guaranteed credit facilities for Customer 10, Customer 11, and Customer 12.

968. On and from 1 March 2016, Crown Melbourne and Crown Perth were aware of the connection between the Chinatown junket and Person 41, who was the ultimate beneficial owner of the Chinatown junket with financial interests in its operations.

Particulars

By at least March 2015, Crown Melbourne and Crown Perth understood that Customer 10 was a junket operator for the Chinatown junket.

On 18 April 2015, Customer 10 transferred money from his Crown Perth DAB account to the Australian bank account of Person 41, who was described to Crown Perth as Customer 10's business partner.

By at least September 2015, Crown Melbourne and Crown Perth were aware that Customer 11 was a relative of Person 41.

By at least September 2015, Crown Melbourne and Crown Perth were "strongly opposed" to Person 41 acting as a guarantor for the junket operator of the Chinatown junket at both Crown Melbourne and Crown Perth.

By at least July 2016, employees of Crown Melbourne and Crown Perth dealt with Person 41 when negotiating the credit limits for Customer 12's credit facility.

Prior to October 2016, Crown Melbourne and Crown Perth understood that Person 41 was the ultimate beneficial owner of the Chinatown junket, along with his spouse, and another individual Person 25 (who was the brother of Customer 12) and his spouse.

Prior to October 2016, Crown's Vice President (International Customer Services) understood Person 41 to be the "boss" of the Chinatown junket and the Chief Legal Officer was aware of the connection between Person 41 and the Chinatown junket.

969. On and from 1 March 2016, the provision of designated services by Crown Melbourne and Crown Perth to junket operators who were part of the Chinatown junket posed higher ML/TF risks due to the connection between the Chinatown junket and Person 41 in circumstances where Crown Melbourne and Crown Perth were aware of:

a. law enforcement interest in Person 41's alleged criminal activities; and

Particulars

On 4 April 2015 and 13 April 2017, Australian taxation authorities requested copies of gaming records for Person 41 from Crown.

On 27 June 2017, law enforcement requested gaming and junket records for Person 41 from Crown Perth.

From August 2017, law enforcement had made various requests to Crown in relation to an investigation into Person 41. Law enforcement had intelligence that Person 41 was closely involved in large-scale junket tours, including the Chinatown junket which operated within Crown and other casinos in Australia, was known colloquially as 'Mr Chinatown', and was a close associate of Customer 26 and Customer 46. The law enforcement investigation concluded that Person 41, along with others, was involved in laundering money for serious organised crime groups.

By August 2019, Crown became aware of media reports that reported that overseas court records recorded that authorities in 2013 had alleged that Person 41 was involved in a serious criminal multi-million dollar fraud scheme, organised crime-type extortion and standover tactics, and arranged for acid to be thrown in a rival's face. Around

this time, Person 41 absconded prior to facing charges, and was subject to an international arrest warrant issued, but was able to enter Australia despite the warrant.

In January 2020, Person 41 was arrested and extradited to an overseas country for suspected money laundering and corruption.

b. publicly available information in relation to Person 41.

Particulars

In October 2016, Crown became aware of an Australian media article that alleged that Person 41 was Crown's "biggest junket", and that it was unclear how Person 41 built the Chinatown junket "gambling empire".

On 23 July 2019, Crown Resorts was asked by an Australian media outlet whether it was aware of open source material that alleged that Person 41 had been accused of serious organised criminal conduct and was wanted by foreign law enforcement authorities since 2011.

By 28 July 2019, Crown became aware of a broadcast programme that referred to Person 41 as "Crown's most lucrative Melbourne junket operator" and as the "single biggest junket operator in Australia".

By August 2019, Crown became aware of Australian media articles that alleged that Person 41:

- operated the Chinatown junket;
- was the subject of overseas legal proceedings for extortion, stand-over tactics, and misappropriating huge amounts of money;
- was the business partner of Customer 26, who was implicated in sex trafficking;
- headed several foreign government-aligned organisations in Melbourne;
- was an "international criminal fugitive, the subject of an Interpol Red Notice for financial crime"; and
- was the subject of law enforcement investigation for international money laundering, which on 17 August 2016 led to a search of a private jet at an Australian airport that Person 41 and their business partner, Customer 46 had boarded.

970. At all relevant times, the provision of designated services by Crown Melbourne and Crown Perth to junket operators who were part of the Chinatown junket posed higher ML/TF risks including because:

a. the table 3, s6 designated services provided to junket operators who were part of the Chinatown junket involved high turnover at Crown Melbourne and Crown Perth;

i. the total turnover from recorded gaming activity on junket programs run by junket operators associated with the Chinatown junket at Crown Melbourne and Crown Perth was approximately $8,101,689,353, comprising:

– approximately $5,975,063,231 at Crown Melbourne;

– approximately $2,126,626,122 at Crown Perth;

b. key players on junket programs run by Chinatown junket operators had high losses at Crown Melbourne and Crown Perth.

i. by 1 March 2016, reported losses by key players on junket programs run by Customer 10 and Customer 11 amounted to approximately $118,365,478; and

ii. on and from 1 March 2016, reported losses by key players on junket programs run by Customer 14, Customer 12, Customer 13 and Customer 11 amounted to approximately $72,672,674 and HKD909,890'

c. Chinatown junket operators were involved in a number of large and unusual third party transactions;

i. by 1 March 2016, total reported incoming third party transactions involving key players on junket programs run by Customer 10 and Customer 11 amounted to approximately $94,985,713 and HKD23,548,964;

ii. by 1 March 2016, total reported outgoing third party transactions involving key players on junket programs run by Customer 10 and Customer 11 amounted to approximately $47,127,086.60 and HKD8,012,410;

iii. on and from 1 March 2016, total reported incoming third party transactions involving key players on junket programs run by Customer 11, Customer 12, Customer 13 and Customer 14 amounted to approximately $12,719,664; and

iv. on and from 1 March 2016, total reported outgoing third party transactions involving key players on junket programs run by Customer 11, Customer 12, Customer 13 and Customer 14 amounted to approximately $15,380,000.

971. On multiple occasions, Crown Melbourne made the Crown private jet available to junket operators who were part of the Chinatown junket. There were inadequate controls on the carrying of large amounts of cash on Crown's private jets.

Particulars

Crown Melbourne provided the Chinatown junket with a Crown private jet at the junket's request on:

- 17 May 2016, for 9 people from an overseas country to Melbourne;
- 24 May 2016, for 6 people from Melbourne to an overseas country;
- 24 June 2016, for 10 people from Melbourne to Perth;
- 27 June 2016, for 12 people from Perth to Melbourne;
- 2 July 2016, for 8 people from Brisbane to Melbourne;
- 3 July 2016, for 8 people from Melbourne to Brisbane;

- 12 July 2016, for 7 people from Melbourne to Perth;
- 16 July 2016, for 6 people from Perth to Melbourne;
- 12 August 2016, for 6 people from an overseas country to Melbourne;
- 17 August 2016, for 4 people from Gold Coast to Melbourne;
- 24 August 2016, for 8 people from Perth to Sydney;
- 24 August 2016, for 5 people from Perth to an overseas country;
- 19 September 2016, for 2 people from Melbourne to an overseas country; and
- 28 September 2016, for 2 people from an overseas country to Melbourne.

See paragraphs 454 and 491(c).

Customer 10

972. Customer 10 was a customer of Crown Melbourne between 26 February 2007 and approximately 22 January 2021.

973. From at least 26 February 2007, Crown Melbourne provided Customer 10 with designated services within the meaning of table 1 and table 3, s6 of the Act.

974. From at least 26 February 2007, Customer 10 received designated services as a junket operator for the Chinatown junket, as a junket representative and as a junket player at Crown Melbourne.

Particulars to paragraphs 973 and 974

On 26 February 2007, Crown Melbourne opened a DAB account and safekeeping account (AUD/HKD) for Customer 10 under a PID.

On 24 August 2014, Crown Melbourne entered into a NONEGPRA with Customer 10 to operate junkets at Crown Melbourne for the Chinatown junket. Between 2014 and 2015, Customer 10 facilitated at least 13 junkets at Crown Melbourne.

Customer 10 was a junket representative for Person 39, who was associated with the Chinatown junket.

Customer 10 received designated services as a junket player under his own junket program and the Customer 11 junket, which was also part of the Chinatown junket.

On 23 October 2014, Crown Melbourne opened an additional DAB account and safekeeping account (AUD/HKD) for Customer 10 under a different PID.

On 29 September 2014, Crown Melbourne opened a credit facility in Customer 10's name (AUD/HKD). On 17 July 2017, Crown Melbourne closed this credit facility.

On 20 January 2021, the Crown Resorts POI Committee considered Customer 10, who had come the Committee's attention through the ILGA inquiry, and agreed to issue a WOL in respect of Customer 10.

The ML/TF risks posed by Customer 10

975. By 1 March 2016, higher ML/TF risks were indicated by the nature and purpose of Customer 10's business relationship with Crown Melbourne as a junket operator linked to the Chinatown junket, his connections to other junket operators and representatives associated with the Chinatown junket (including Person 41) the nature of the transactions he had been conducting, together with the suspicions Crown Melbourne itself had formed with respect to Customer 10.

Particulars

Section 36(1)(a), (b) of the Act and Chapter 15 of the Rules.

Between 2014 and 2015, Customer 10 was a junket operator, junket representative and junket player. He received designated services through the channel of junket programs. This channel lacked transparency: see paragraph 477.

Links to Chinatown junket

By March 2015, Crown Melbourne was aware that Customer 10 was connected to the Chinatown junket and, as a result, also connected to Person 41 who was the ultimate beneficial owner behind the junket: see paragraphs 968 and 969. Crown management began to refer to the junket operations run by Customer 10 as the 'Chinatown' junket.

Customer 10's junket representatives included Person 23 and Person 40, who also represented other junket operators linked to the Chinatown junket.

Junket activity

By 1 March 2016, Customer 10 had operated approximately 32 junket programs at Crown Melbourne and Crown Perth for a total of 159 key players.

By the end of 2016, Crown Melbourne recorded gaming activity on junket programs operated by Customer 10 as having turnover of $3,943,109,344 with losses of $83,011,938. Commissions of $43,744,008 were payable by Crown Melbourne to Customer 10.

By 1 March 2016, Crown management approved a credit facility for Customer 10's junket programs, up to limits of between AUD$20,000,000 and AUD$50,000,000. The credit facility was subject to a guarantee from an individual associated with the Chinatown junket, Person 39 (who subsequently provided guarantees to other junket operators who were part of the Chinatown junket), which was re-executed prior to issuing credit markers to Customer 10. Between 2014 and 2015, $769,502,469 was deposited into Customer 10's credit facility.

On 2 December 2014, Customer 10's junket representative exchanged $500,000 of gaming chips for cash, and the following day, Customer 10's junket representative, Person 40, deposited $300,000 into Customer 10's DAB account which was withdrawn via telegraphic transfer to a third party: SMR dated 4 December 2014.

In July 2015, Customer 10 transferred funds from his DAB account to Customer 1's DAB account at a time when a key player was noted under junket programs run by both Customer 10 and Customer 1.

Suspicious third party transactions

Between 18 November 2014 and 30 June 2015, Customer 10 made telegraphic transfers to third party individuals totalling at least $10,341,426.

Between 21 October 2014 and 15 October 2015, Customer 10 made telegraphic transfers to third party companies totalling at least $8,146,748.

Between 26 November 2014 and 22 September 2015, Customer 10 received telegraphic transfers into his DAB account from third parties, totalling at least $2,483,936.

Change of Chinatown junket operator – October 2015

In October 2015, Crown management, including the CEO (Australian Resorts) was aware and approved of Customer 11 replacing Customer 10 as the operator of the Chinatown junket at Crown. Crown management understood that this would involve transferring the Chinatown junket's credit arrangements with Crown, which were in Customer 10's name, to Customer 11.

On 15 October 2015, $11,944,467 was transferred from Customer 10's DAB account to Customer 11's DAB account: SMR dated 16 October 2015.

Law enforcement

In 2015, Crown Melbourne received a law enforcement request for records in relation to Customer 10.

SMRs

By 1 March 2016, Crown Melbourne had given the AUSTRAC CEO 22 SMRs in relation to Customer 10. The SMRs reported:

- telegraphic transfers to and from Customer 10's DAB account to and from unrelated third parties;
- suspicious conduct by Customer 10's junket representatives; and
- suspicious transfers between Customer 10 and Customer 1.

Other red flags

On 5 June 2015, HKD36,120,000 was received into Customer 10's DAB at City of Dreams, with a direction to send the funds via

telegraphic transfer to Crown Melbourne to be used to repay a credit marker. This transaction appears to relate to the City of Dreams deposit service: see paragraphs 332ff and 334ff.

By 1 March 2016, Customer 10's transactions involved repeated transactions indicative of ML/TF typologies that were not detected prior to lookbacks in 2021 and 2022 (see SMRs dated 22 November 2021 and 6 January 2022), including by an independent auditor in 2021 as follows: see paragraph 686 and 687.

ML-TF typology – layering

Between 2007 and 2021, Customer 10 engaged in the following transactions at Crown Melbourne, indicative of the ML/TF typology of layering in order to make it difficult to determine the source or legitimacy of funds (SMR dated 10 January 2022):

- 17 sub-threshold cash deposits totalling $80,724;
- 15 sub-threshold cash withdrawals totalling $68,845;
- 45 threshold cash ins (across his deposit and safekeeping account or cash table games buy-ins) totalling $4,501,456.11;
- 329 threshold cash-outs totalling $18,594,909.46 (either from his DAB account or safekeeping account, or chip cash-outs);
- 64 incoming telegraphic transfers totalling $88,885,713; and
- 31 outgoing telegraphic transfers totalling $43,916,592.60.

Between 2 November 2014 and 11 September 2015, Customer 10 engaged in 11 specific suspicious transactions involving the deposit and withdrawal of cash and telegraphic transfers, indicative of the ML/TF typology of layering in order to make it difficult to determine the source or legitimacy of funds. These included (SMR dated 22 November 2021):

- on 2 November 2014, $50,000 in cash was deposited into Customer 10's DAB account at Crown Melbourne by Customer 10's junket representative, then withdrawn as a telegraphic transfer to a key player, who did not have recorded ratings suggesting he did not play on any of the junkets;
- on 17 April 2015, $95,000 in cash was withdrawn from Customer 10's DAB account by Customer 10's junket representative, Person 58, then over the next two days, $83,300 cash deposited back in and $12,000 was withdrawn;
- on 21 May 2015, another junket operator at Crown who had played on Customer 10's junket transferred HKD4,470,036 into Customer 10's DAB account, despite recording wins in AUD and losses in HKD;
- on 22 July 2015, Customer 10's junket representative Person 23 withdrew $100,000 in cash from Customer 10's DAB account,

then 4 hours later, deposited $100,000 in cash, then 5 hours later, withdrew $50,000 in cash again;

- on 23 July 2015, $8,248,000 in junket program chips, which did not appear to be winnings, were deposited into Customer 10's DAB account, then withdrawn via telegraphic transfer to Customer 10's DAB account at another Australian casino;
- on 24 July 2015, Customer 10's junket representative Person 23 withdrew $90,000 in cash from Customer 10's DAB account;
- on 31 July 2015, Customer 10's junket representative, Person 58, withdrew $150,000 in cash from Customer 10's DAB account, then withdrew a further $57,000 the following day;
- on 24 August 2015, Customer 10's junket representative Person 23 withdrew $30,000 from Customer 10's DAB account, then one hour later cashed out $30,000 in chips, then 2 hours later withdrew a further $50,000 in cash. Customer 10's other junket representative, Person 58, deposited $30,000 back into Customer 10's DAB account;
- on 24 August 2015, $2,423,700 was deposited into Customer 10's junket safekeeping account, then 15 minutes later $2,424,112 was withdrawn from that account via telegraphic transfer to a third party, Person 39 (this individual guaranteed Customer 10's credit lines at Crown);
- on 10 September 2015, four telegraphic transfers of $380,000, $360,000, $300,000 and $23,936, totalling $1,063,936 from an overseas money remittance service were deposited into Customer 10's DAB account; and
- on 11 September 2015, the same amount $1,063,936 was withdrawn via telegraphic transfer to Customer 10's DAB account at another Australian casino.

Between 2014 and 2015, Customer 10 transacted through his DAB account on an almost daily basis, with the longest period of non-activity being 12 days.

Between 2014 and 2015, Customer 10 transferred funds from his DAB account to his safekeeping account on 36 occasions, to a total of $145,754,380, which were held on average for eight days before a withdrawal was made. During this period, a minimum balance of $1,000,000 was maintained before all funds were withdrawn on 15 October 2015.

Between 2014 and 2015:

- the total value of the 925 deposits into Customer 10's DAB account was $2,331,510,812; and
- the total value of the 1,111 withdrawals from Customer 10's DAB account was $2,331,510,266.

ML/TF typology – quick turnovers

Between 20 October 2014 and 11 September 2015, Customer 10 engaged in 10 transactions that were responsive to the ML/TF typology of quick turnovers, in which $10,012,144 was deposited and $27,121,994 subsequently withdrawn.

ML/TF typology – third party transactions

Between 2014 and 2015, Customer 10 received 74 telegraphic transfers from third parties, of which 27 related to an individual and 47 related to a legal entity:

- of the telegraphic transfers received from individuals, six out of 27 were from key players on Customer 10's junkets, and one was received from Person 41, who was subsequently extradited to a foreign country on charges of suspected money laundering and corruption; and
- of the telegraphic transfers received from the 47 legal entities, five entities had sent or received funds from 15 Crown patrons between October 2014 to October 2015, and three entities had been deregistered as at September 2021.

Due diligence

By 1 March 2016, the due diligence steps taken with respect to Customer 10 were as follows.

On 30 October 2012, 26 August 2014, and 26 August 2015 Crown Melbourne performed a risk intelligence searches on Customer 10, which returned a match to Customer 10 related to organised crime, but Crown Melbourne reached a conclusion that it was unlikely to be Customer 10.

By October 2014, Crown was informed by an overseas Crown employee that Customer 10 was a general manager of a property management and building materials sales company.

On 2 September 2015, Crown obtained a wealth report on Customer 10 which confirmed that was Customer 10's occupation.

976. As at 1 March 2016, Customer 10 should have been recognised by Crown Melbourne as a high risk customer for the reasons pleaded at paragraph 975.

Particulars

Section 36(1)(a), (b) of the Act and Chapter 15 of the Rules.

977. At all times on and from 1 March 2016, Customer 10 should have been recognised by Crown Melbourne as a high risk customer by reason of the matters pleaded at paragraphs 975, 979, 980, 981 and 982.

Particulars

Section 36(1)(a), (b) of the Act and Chapter 15 of the Rules.

978. It was not until 20 January 2021 that Customer 10 was rated high risk by Crown Melbourne.

Particulars

On 39 occasions between 9 May 2014 and 16 October 2015, Crown Melbourne assessed Customer 10 as moderate risk.

On 23 October 2015 and 28 October 2015, Crown Melbourne assessed Customer 10 as significant risk.

On 25 September 2017, Crown Melbourne assessed Customer 10 as moderate risk.

See paragraph 481.

979. On and from 1 March 2016, designated services provided to Customer 10 posed higher ML/TF risks including because the provision of designated services to Customer 10 involved a combination of the following factors:

a. Customer 10 received high value financial services (table 1, s6) and high value gaming services (table 3, s6), through multiple junket programs: see paragraph 473ff;

b. Customer 10 was a junket operator of the Chinatown junket, a junket representative for the Chinatown junket and a junket player (including on the Chinatown junket);

c. by March 2015, as a result of Customer 10's connection to the Chinatown junket, Crown Melbourne knew that Customer 10 was linked to Person 41 who was understood to be the ultimate beneficial owner of the Chinatown junket. This connection presented higher ML risks for the reasons set out at paragraphs 968 and 969;

d. these transactions took place against the background of:

i. by 1 March 2016, Customer 10 had operated approximately 32 junket programs at Crown Melbourne and Crown Perth for a total of 159 key players;

ii. by 1 March 2016, turnover on junket programs operated by Customer 10 at Crown Melbourne had exceeded $3,943,109,344;

iii. Crown Melbourne was aware of suspicious transactions between Customer 10 and Customer 1, involving third parties who played on both Chinatown and Suncity junkets;

iv. Customer 10 was provided with significant amounts of credit upon request, up to limits of between AUD$20,000,000 and AUD$50,000,000: see paragraphs 280ff and 487;

v. law enforcement and AUSTRAC having expressed an interest in Customer 10 on two occasions in 2015;

vi. transactions involving Customer 10, his junket representatives and key players involved repeated transactions indicative of ML/TF typologies that were not detected prior to lookbacks in 2021 and 2022, including layering, quick turnover of funds (without betting) and cashing-in large value chips without recorded gameplay: see paragraph 24; and

vii. 22 SMRs in relation to Customer 10 being given to the AUSTRAC CEO by Crown Melbourne by 1 March 2016.

e. by reason of the matters pleaded at subparagraphs a. to d., and in light of his connections to the Chinatown junket, there were real risks that Customer 10's source of wealth/funds were not legitimate.

Monitoring of Customer 10's transactions

980. At no time did Crown Melbourne appropriately monitor Customer 10's transactions on a risk-basis.

Particulars

Section 36(1)(a), (b) of the Act and rules 15.4 to 15.8 of the Rules..

Crown Melbourne was unable to monitor the ML/TF risks posed by transactions associated with Customer 10's junkets appropriately, including transactions by his junket representatives and key players on his junkets because it did not make and keep appropriate records of designated services provided: see paragraphs 483ff.

Crown Melbourne did not apply appropriate risk-based transaction monitoring to designated services provided to Customer 10: see paragraphs 590ff and 629 to 642 (designated services) and 643 to 649 (transactions facilitated through junkets).

Lookback

Customer 10's transactions involved repeated transactions indicative of ML/TF typologies and vulnerabilities that were not detected prior to a 2021 lookback. Had appropriate risk-based transaction monitoring been applied, these transactions could have been identified earlier: see paragraphs 686 and 687.

On 15 October 2021, transactions involving Customer 10 were identified by an independent auditor as indicative of the ML/TF typologies of layering, structuring, smurfing, and quick turnovers of money and the risk area of junket-related activity. The independent auditor also performed a deep dive review of Customer 10's activities.

Ongoing customer due diligence

981. On and from 1 March 2016, on multiple occasions, the provision of designated services to Customer 10 at Crown Melbourne raised red flags indicative of higher ML/TF risks as a result of Customer 10's connection to Person 41 as a business partner and through the Chinatown junket.

Particulars

Section 36(1)(a), (b) of the Act and Chapter 15 of the Rules.

By 1 March 2016, Crown Melbourne and Crown Perth were aware that Person 41 was the ultimate beneficial owner and controller behind the Chinatown junket operations at Crown, including through Customer 10, and had financial interests in the business of the Chinatown junket: see particulars to paragraphs 968 and 969.

February 2021 – Bergin Report

The Bergin Report found that prior to October 2016, Crown management was aware that Person 41 was a "financier" and "boss" of a number of Chinatown-branded junkets run at both Crown Melbourne and Crown Perth, including by Customer 10. The Bergin Report described junket operators including Customer 10 as "front men" for the Chinatown junket, and concluded that Crown did not have a real or proper understanding of these individuals to be satisfied they were of good repute.

982. On and from 1 March 2016, on multiple occasions, the provision of designated services to Customer 10 at Crown Melbourne raised red flags reflective of higher ML/TF risks.

Particulars

Section 36(1)(a), (b) of the Act and Chapter 15 of the Rules.

2016

In 2016, Crown Melbourne recorded Customer 10's rated gaming activity as involving buy-in of $900, turnover of $21,643 and losses of $300.

2017

In 2017, Crown Melbourne recorded Customer 10's rated gaming activity as involving buy-in of $9,700, turnover of $21,583 and losses of $7,700.

2018-2021

Between 2018 and 2021, Crown Melbourne recorded no rated gaming activity for Customer 10.

983. At no time did Crown Melbourne undertake appropriate risk-based customer due diligence with respect to Customer 10 with a view to identifying, mitigating and managing the ML/TF risks posed by the provision of designated services on and from 1 March 2016.

a. At no time did Crown Melbourne take appropriate steps to understand whether Customer 10's source of wealth/funds was legitimate, despite Crown Melbourne's knowledge of his connection to the Chinatown junket and Person 41.

b. At no time did Crown Melbourne take appropriate steps to identify or analyse the ML/TF risks of Customer 10's transactions.

c. At no time did Crown Melbourne give appropriate consideration to whether large and high risk transactions should be processed.

d. At no time did Crown Melbourne take appropriate steps to consider Customer 10's relationship with Person 41 as a business partner and through the Chinatown junket and the ML/TF risks arising as a result of that association.

e. At no time did senior management consider whether continuing the business relationship with Customer 10 was within Crown Melbourne's ML/TF risk appetite: see paragraph 668ff.

Particulars

Section 36(1)(a) of the Act.

The due diligence steps taken with respect to Customer 10 included:

Wealth information and database searches

On 4 November 2016, Crown requested a wealth report on Customer 10. Crown was advised that a report could not be compiled based on the information that Crown had provided.

In December 2016, Crown performed risk intelligence and company searches, and obtained updated wealth reports on Customer 10.

Junket profile

In December 2016, the Credit control team drafted a junket profile on Customer 10, performed risk intelligence and company searches, and obtained updated wealth reports on Customer 10.

By 18 November 2019, Crown noted that Customer 10 was "not active" when preparing a list of all junket operators with activity from 2017 onwards.

Between 2014 and 2021, Crown Melbourne failed to appropriately consider the ML/TF risks of the source of Customer 10's wealth/funds or whether an ongoing business relationship with Customer 10 was within their ML/TF risk appetite.

Consideration by Crown Resorts POI Committee

On 20 January 2021, the Crown Resorts POI Committee considered Customer 10, who had come to the Committee's attention through the ILGA inquiry, and issued a WOL against Customer 10. On 22 January 2021, the WOL took effect at Crown Melbourne.

Prior to January 2021, none of these steps were proportionate to the ML/TF risks reasonably posed by Customer 10 on and from 1 March 2016.

984. By reason of the matters pleaded from paragraphs 972 to 983, on and from 1 March 2016, Crown Melbourne:

a. did not monitor Customer 10 in relation to the provision of designated services, with a view to identifying, mitigating and managing the ML/TF risks reasonably faced; and

b. did not do so in accordance with rr15.5 and 15.9 of the Rules.

985. By reason of the matters pleaded at paragraph 984, Crown Melbourne contravened s36(1) of the Act on and from 1 March 2016 to 22 January 2021 with respect to Customer 10.

Particulars

Section 36(1) of the Act is a civil penalty provision: s36(2) of the Act.

Customer 11

986. Customer 11 was a customer of Crown Melbourne from 20 September 2015 to January 2021.

987. From at least 20 September 2015, Crown Melbourne provided Customer 11 with designated services within the meaning of table 1 and table 3, s6 of the Act.

988. From at least 20 September 2015, Customer 11 received designated services as a junket operator for the Chinatown junket at Crown Melbourne.

Particulars to paragraphs 987 and 988

On 27 August 2015, Crown Melbourne entered into a NONEGPRA with Customer 11 to operate junkets at Crown Melbourne.

On 28 August 2015, Crown Melbourne opened a DAB account and safekeeping account (AUD/HKD) for Customer 11 under his first PID.

On 29 September 2015, Crown opened a credit facility for Customer 11 under his first PID. On 21 April 2016, Crown Melbourne closed this credit facility.

On 11 October 2015, Crown Melbourne opened two further DAB account and safekeeping accounts (AUD/HKD) for Customer 11 under his second and third PID.

On 5 November 2015, Crown Melbourne opened a fourth DAB account and safekeeping account (AUD) for Customer 11 under his fourth PID.

Between 10 March 2016 and 22 April 2016, Customer 11 ran approximately ten junket programs at Crown Melbourne, including two under his initial PID, three under his second PID, two under his third PID, one under his fourth PID, and two other programs run under another PID. During this period, Customer 11 had five junket representatives, including Person 23 and Person 40.

Customer 11 was a junket representative for another Chinatown junket operator, Customer 14.

On 20 January 2021, the Crown Resorts POI Committee considered Customer 11, who had come the Committee's attention through the ILGA inquiry, and agreed to issue a WOL in respect of Customer 11.

989. Customer 11 was a customer of Crown Perth from 10 January 2015 to 16 February 2021.

990. From 10 January 2015, Crown Perth provided Customer 11 with designated services within the meaning of table 1 and table 3, s6 of the Act.

991. From at least 20 September 2015, Customer 11 received designated services as a junket operator for the Chinatown junket at Crown Perth.

Particulars to paragraphs 990 and 991

On 27 August 2015, Crown Perth entered into a NONEGPRA with Customer 11 to operate junkets at Crown Perth.

On 10 January 2015, opened a DAB account and safekeeping account (AUD/HKD) for Customer 11 under his first and second PID.

On 29 September 2015, Crown Perth provided Customer 11 with a FAF under his first and second PID. On 11 October 2016, Crown Perth closed this credit facility.

Between 23 March 2016 and 24 April 2016, Customer 11 ran at least one junket program at Crown Perth. During this period, Customer 11 had five junket representatives, including Person 23 and Person 40.

On 20 January 2021, the Crown Resorts POI Committee considered Customer 11, who had come the Committee's attention through the ILGA inquiry, and agreed to issue an NRL in respect of Customer 11.

On 16 February 2021, the NRL took effect at Crown Perth.

The ML/TF risks posed by Customer 11

992. By 1 March 2016, higher ML/TF risks were indicated by the nature and purpose of Customer 11's business relationship with Crown Melbourne and Crown Perth as a junket operator linked to the Chinatown junket, his connections to other junket operators and representatives associated with the Chinatown junket (including Person 41) the nature of the transactions he had been conducting, together with the suspicions Crown Melbourne itself had formed with respect to Customer 11.

Particulars

Section 36(1)(a), (b) of the Act and Chapter 15 of the Rules.

Customer 11 was a junket operator. He received designated services through the channel of junket programs. This channel lacked transparency: see paragraph 477.

Links to Chinatown junket

At the time that Customer 11 applied to be a junket operator, Crown Melbourne and Crown Perth were aware that Customer 11 was connected to the Chinatown junket, and was a family member of Person 41.

Crown management understood that Customer 11 was replacing Customer 10 as the operator of the Chinatown junket at Crown. Crown management also understood that this would involve transferring the Chinatown junket's credit arrangements with Crown, which were in the name of Customer 10 to Customer 11.

Customer 11's junket representatives included Person 23 and Person 40, who also represented other junket operators linked to the Chinatown junket.

Junket activity

By 1 March 2016, Customer 11 had operated approximately 4 junket programs at Crown Melbourne. Crown Melbourne recorded that the total turnover for those programs was $1,212,752,195, with losses of $17,954,290. Commissions of $11,693,119 were payable by Crown Melbourne to Customer 11.

By 1 March 2016, Customer 11 had operated approximately 5 junket programs at Crown Perth. Crown Perth recorded that the total turnover for those programs was $895,775,300, with losses of $15,311,890. Commissions of $11,060,769 were payable by Crown Perth to Customer 11.

By 1 March 2016, Crown management approved numerous credit facilities for Customer 11's junkets prior to the junket programs in various amounts ranging from $40,000,000 to $60,000,000. From December 2015, Crown management approved a standing credit line of $60,000,000 for Customer 11's junkets.

However, Crown was reluctant to approve credit for Customer 11 due to concerns about his creditworthiness. On 10 September 2015, the Credit control team were informed that a similar proposal to change Chinatown's credit arrangements at another Australian casino had been rejected because the casino was not comfortable giving Customer 11 credit, due to the limited information they had about him for credit purposes.

Crown was opposed to Person 41 acting as guarantor, however agreed to accept a guarantee from other individuals associated with the Chinatown junket, Person 25 and Person 39, who subsequently provided guarantees to other Chinatown junket operators.

Suspicious third party transactions

On 14 October 2016, Customer 11 arranged for a telegraphic transfer of $2,000,000 from his Crown Melbourne DAB account to a third party Australian company.

On 15 October 2015, Customer 11 arranged for a telegraphic transfer of $312,318 from his Crown Melbourne DAB account to a third party Australian company.

On 27 October 2015, a telegraphic transfer of $50,000 was received into Customer 11's Crown Melbourne DAB account from a third party, Person 19, who was not a key player under any of Customer 11's junkets.

On 4 November 2015, Crown Melbourne received two payments of $200,000 and $300,000 from a third party company for the benefit of Customer 11. The Credit control team investigated the company and confirmed it was a money changer, and the Senior Vice President (International Business) approved acceptance of the funds.

On 30 November 2015, Customer 11 arranged for a telegraphic transfer of $1,500,000 from his Crown Melbourne DAB account to a third party.

On 7 January 2016, Customer 11 arranged for a telegraphic transfer of HKD7,320,000 from his Crown Melbourne DAB account to a key player under Customer 11's junket, which was much larger that the player's noted win under the junket.

On 28 January 2016, Customer 11 arranged for a telegraphic transfer of $4,483,000 from his Crown Melbourne DAB account to a key player under Customer 11's junket, despite the player having lost under recent junket programs.

SMRs

By 1 March 2016, Crown Melbourne had given the AUSTRAC CEO 13 SMRs in relation to Customer 11, which reported:

- losses noted for the key players under Customer 11's junket programs;
- a suspicious transfer of $11,944,467 between two Chinatown junket operators, Customer 10 and Customer 11; and
- suspicious telegraphic transfers from Customer 11's Crown Melbourne DAB account, including to unrelated third parties.

Other red flags

At various times, Customer 11 held large sums in his DAB accounts with Crown Melbourne. As at 30 November 2015, Customer 11 held $23,710,105 in his deposit account with Crown Melbourne. A further $22,833,805 was held in a safekeeping account.

Due diligence

By 1 March 2016, the only due diligence steps taken with respect to Customer 11 were risk intelligence searches in September 2015.

993. As at 1 March 2016, Customer 11 should have been recognised by Crown Melbourne as a high risk customer for the reasons pleaded at paragraph 992.

Particulars

Section 36(1)(a), (b) of the Act and Chapter 15 of the Rules.

994. At all times on and from 1 March 2016, Customer 11 should have been recognised by Crown Melbourne as a high risk customer by reason of the matters pleaded at paragraphs 992, 999, 1001, 1002, 1003, and 1005.

Particulars

Section 36(1)(a), (b) of the Act and Chapter 15 of the Rules.

995. It was not until 20 January 2021 that Customer 11 was rated high risk by Crown Melbourne.

Particulars

On 15 occasions between 11 September 2015 and 29 May 2019, Crown Melbourne rated Customer 11 low risk.

Crown Melbourne did not assess Customer 11's risk as high until 20 January 2021.

See paragraph 481.

996. As at 1 March 2016, Customer 11 should have been recognised by Crown Perth as a high risk customer for the reasons pleaded at paragraph 992.

Particulars

Section 36(1)(a), (b) of the Act and Chapter 15 of the Rules.

997. At all times on and from 1 March 2016, Customer 11 should have been recognised by Crown Perth as a high risk customer by reason of the matters pleaded at paragraphs 992, 999, 1001, 1002, 1003, and 1008.

Particulars

Section 36(1)(a), (b) of the Act and Chapter 15 of the Rules

998. It was not until 20 January 2021 that Crown Perth rated Customer 11 high risk.

Particulars

On 4 occasions between 11 August 2016 and 31 October 2017, Crown Melbourne assessed Customer 11 as low risk.

On 10 November 2017 and 12 January 2019, Crown Perth assessed Customer 11 as significant risk.

Crown Melbourne did not assess Customer 11's risk as high until 20 January 2021.

See paragraph 481.

999. On and from 1 March 2016, designated services provided to Customer 11 posed higher ML/TF risks including because the provision of designated services to Customer 11 involved a combination of the following factors:

a. Customer 11 was a junket operator of the Chinatown junket;

b. by August 2015, Crown Melbourne knew that Customer 11 was linked to Person 41 who was understood to be the ultimate beneficial owner of the Chinatown junket, both as a junket operator for the Chinatown junket and as Person 41's relative. This connection presented higher ML risks for the reasons set out at paragraphs 968 and 969;

c. Customer 11 received high value financial services (table 1, s6) and gaming services (table 3, s6), through multiple junket programs: see paragraph 473ff;

d. Customer 11 was a junket operator who facilitated the provision of high value financial and gaming services (tables 1 and 3, s6) to key players (including foreign PEPs) on his junket programs: see paragraph 473ff;

e. by 30 June 2016, total turnover at Crown Melbourne for junket programs operated by Customer 11 had exceeded $1,217,764,090;

f. by 30 June 2016, total turnover at Crown Perth for junket programs operated by Customer 11 had exceeded $1,547,848,500;

g. designated services provided to Customer 11 lacked transparency as the services were provided through the channel of junket programs: see paragraph 477(e);

h. the table 3, s6, designated services provided to Customer 11 involved high turnover;

i. Customer 11 regularly made transfers to or received transfers from third parties, including third parties in respect of whom suspicions had been formed, and including to other junket operators including Customer 2 and Customer 10;

j. designated services provided to Customer 11 involved large cross-border movements of funds: see paragraph 238(d);

k. Customer 11 made or received large transfers and unusual requests for transfers to and from other Australian and overseas casinos: see paragraphs 398ff and 407ff;

l. at various times, Customer 11 was provided with a significant amount of credit up to limits of $80,000,000;

m. Customer 11 engaged in other transactions indicative of ML/TF typologies and vulnerabilities, including cashing-in large value chips with no evidence of play: see paragraph 24;

n. these transactions took place against the background of:

   i. 13 SMRs being given to the AUSTRAC CEO by 1 March 2016; and

   ii. at least AUD$550,000 in third party deposits received into Customer 11's DAB account by 1 March 2016; and

   iii. at least AUD$8,295,318 and HKD7,320,000 in third party withdrawals from Customer 11's DAB account by 1 March 2016;

o. in October 2017, Crown Perth was advised that Customer 11 was of interest to the Western Australian gambling regulator;

p. in September and October 2020, media reports named Customer 11 as a person involved in drug dealing and money laundering; and

q. by reason of the matters pleaded at subparagraphs a. to p., and in light of his connections to the Chinatown junket, there were real risks that Customer 11's source of wealth/funds were not legitimate.

Monitoring of Customer 11's transactions

1000. At no time did Crown Melbourne appropriately monitor Customer 11's transactions on a risk-basis.

Particulars

Section 36(1)(a), (b) of the Act and rules 15.4 to 15.8 of the Rules..

Crown Melbourne was unable to monitor the ML/TF risks posed by the transactions associated with Customer 11's junkets appropriately, including transactions by his junket representatives and key players on his junkets, because it did not make and keep appropriate records of designated services provided: see paragraphs 483ff.

Crown Melbourne did not apply appropriate risk-based transaction monitoring to designated services provided to Customer 11: see paragraphs 590ff and 629 to 642 (designated services) and 643 to 649 (transactions facilitated through junkets).

Ongoing customer due diligence

1001. On and from 1 March 2016, on multiple occasions, the provision of designated services to Customer 11 at Crown Melbourne raised red flags reflective of higher ML/TF risks as a result of Customer 11's connection to Person 41 as a relative and through the Chinatown junket.

Particulars

Section 36(1)(a), (b) of the Act and Chapter 15 of the Rules.

2016

By 1 March 2016, Crown Melbourne and Crown Perth were aware that Person 41 was the ultimate beneficial owner and controller behind the Chinatown junket operations at Crown, including through Customer 11, and had financial interests in the business of the Chinatown junket: see particulars to paragraphs 968 and 969.

2020

Between September and October 2020, media reports noted that Customer 11:

- was involved in operating the Chinatown junket along with other operators;
- had sent $500,000 from his Crown Perth DAB account to a drug dealer described as a 'good friend' of the Chinatown junket in 2017;
- had commenced proceedings against Customer 51, an associate of Customer 40, over a gambling chip debt;
- had been allegedly arrested over money laundering offences in 2012; and
- was allegedly a convicted drug dealer.

February 2021 – Bergin Report

The Bergin Report found that prior to October 2016, Crown management was aware that Person 41 was a "financier" and "boss" of a number of 'Chinatown'-branded junkets run at both Crown Melbourne and Crown Perth, including by Customer 11. The Bergin Report described junket operators including Customer 11 as "front men" for the Chinatown junket and Person 41, and concluded that Crown did not have a real or proper understanding of these individuals to be satisfied they were of good repute.

1002. On and from 1 March 2016, on multiple occasions, the provision of designated services to Customer 11 at Crown Melbourne and Crown Perth raised red flags reflective of higher ML/TF risks arising from Customer 11's junket activity.

Particulars

Junket activity in 2016

During the 2016 financial year, Crown Melbourne recorded gaming activity on junket programs run by Customer 11 as having turnover of

$1,217,764,090, with losses of $7,069,456. Commissions of $11,643,849 were payable by Crown Melbourne to Customer 11.

During the 2016 financial year, Crown Perth recorded gaming activity on junket programs run by Customer 11 at Crown Perth as having turnover of $1,547,848,500 with losses of $31,791,306. Commissions of $11,060,769 were payable by Crown Perth to Customer 11.

On 7 April 2016, Crown management agreed to reapprove Customer 11's credit limit of $80,000,000 for his credit facility. By 21 April 2016, Crown Melbourne had closed Customer 11's credit facility.

Crown Melbourne was aware of the high losses noted for eight key players under Customer 11's junkets at Crown Melbourne totalling AUD$3,712,900 and HKD909,890.

1003. On and from 1 March 2016, on multiple occasions, the provision of designated services to Customer 11 at Crown Melbourne and Crown Perth raised red flags reflective of higher ML/TF risks as a result of unusual transactions, including suspicious cash transactions, involving Customer 11 and his junket representatives and key players.

Particulars

See paragraphs 420ff, 450, 451, 456ff and 491.

Unusual transactions in 2016

On 22 March 2016, a telegraphic transfer of $50,000 was deposited into Customer 11's Crown Melbourne DAB account from a third party, who was not listed under any of Customer 11's junket programs: SMR dated 23 March 2016 (Crown Melbourne).

On 26 March 2016, a key player who had a high turnover and wins of $1,400,000 on Customer 11's junket at Crown Perth deposited funds, then withdrew a CPV from Customer 11's Crown Melbourne DAB account: SMR dated 31 March 2016 (Crown Melbourne).

On 26 April 2016, Crown Melbourne received a payment from another Australian casino of $1,076,047 for Customer 11. On 24 May 2016 and 25 May 2016, a third party company based in Australia with overseas-based shareholders transferred AUD$4,980,000 and AUD$710,000 to Crown Perth for the benefit of Customer 11. It appears that these funds were accepted by Crown Perth in satisfaction of an outstanding credit marker by Customer 11.

On 23 November 2016, Customer 11 sent a telegraphic transfer in foreign currency equivalent to AUD$3,000,000 to an overseas casino. The order form submitted for the transfer shows the payee as Person 41 crossed out and amended to Person 19, a key player on Customer 11's junkets. A subsequent AML team investigation reported by Crown on 18 January 2021 determined that the change in reference was unlikely to be suspicious because of the operational connections between Customer 11, Person 41 and Person 19.

On 17 November 2016, Customer 11 withdrew $1,000,000 from his Crown Perth DAB account and requested that the funds be sent to

the Crown Melbourne DAB account of another junket operator, Customer 2, by telegraphic transfer: SMR dated 22 November 2016 (Crown Perth).

Unusual transactions in 2017

On 12 January 2017, Customer 11 instructed Crown Perth to transfer $500,000 from his Crown Perth DAB account to a third party, who was not a key player or a patron of Crown Perth: SMR dated 20 January 2017.

On 15 January 2017, Customer 11 instructed Crown Perth to transfer $500,000 from Customer 11's Crown Perth DAB account to a third party, Person 24: SMR dated 3 November 2017. The transaction was processed on 16 January 2017.

On 31 October 2017, the Western Australian gaming regulator issued a request for information regarding the transaction on 16 January 2017 involving Customer 11 and Person 24.

Unusual transactions in 2019

On 28 May 2019, Customer 11 was acting as a junket representative for Customer 14. Another of Customer 14's junket representatives, Person 27, had arranged for a telegraphic transfer of $100,000 from his bank account to his Crown account, then exchanged the funds for gaming chips (3x $25,000; 4x $5,000). Customer 11 then came to the Crown Melbourne Cage and presented the gaming chips in the same breakdown and requested to exchange the chips for cash. When questioned about the provenance of the gaming chips, Customer 11 said that they belonged to Person 2, a key player on Customer 14's junket in January 2019. Crown declined to process the transaction as there was no evidence that the Person 2 owned the chips. Crown Melbourne returned the chips to Customer 11: SMR dated 28 May 2019 (Crown Melbourne).

1004. At no time did Crown Melbourne or Crown Perth undertake appropriate risk-based customer due diligence with respect to Customer 11 with a view to identifying, mitigating and managing the ML/TF risks posed by the provision of designated services on and from 1 March 2016.

a. At no time did Crown Melbourne or Crown Perth take appropriate steps to understand whether Customer 11's source of wealth/funds was legitimate, despite Crown Melbourne's knowledge of his connection to the Chinatown junket and Person 41.

b. At no time did Crown Melbourne or Crown Perth take appropriate steps to identify or analyse the ML/TF risks of Customer 11's transactions or to consider whether they had a lawful purpose.

c. With the exception of the decision to refuse to exchange gaming chips for cash in May 2019, at no time did Crown Melbourne or Crown Perth give appropriate consideration to whether large and high risk transactions should be processed.

d. At no time did Crown Melbourne take appropriate steps to consider Customer 11's relationship with Person 41 as a relative and through the Chinatown junket and the ML/TF risks arising as a result of that association.

e. On each occasion prior to January 2021 that senior management considered whether to continue the business relationship with Customer 11, senior management failed to give adequate consideration to whether the ML/TF risks posed by Customer 11 were within Crown Melbourne or Crown Perth's risk appetite.

Particulars

Section 36(1)(a) of the Act.

The due diligence steps taken with respect to Customer 11 were as follows.

Database searches

In December 2016, Crown Melbourne and Crown Perth relied on a risk intelligence search for Customer 11.

Senior management consideration

Following the Western Australian gaming regulator's enquiry about the transaction on 16 January 2017 involving Customer 11 and Person 24, the Crown Perth Fortnightly AML/CTF Officer Meeting on 10 November 2017 considered Customer 11's risk and increased it to significant.

Following a review by the Fortnightly AML/CTF Officer Meeting at Crown Perth in December 2018, on 12 January 2019, the Group General Manager – AML determined that Customer 11's risk rating should remain at significant.

On 20 January 2021, the Crown Resorts POI Committee considered Customer 11, who had come to the Committee's attention through the ILGA inquiry, which issued a withdrawal of license against Customer 11, which was applied by Crown Melbourne on 22 January 2021.

Prior to January 2021, none of these steps were proportionate to the ML/TF risks reasonably posed by Customer 11.

Enhanced customer due diligence

1005. Having formed a suspicion for the purposes of s41 of the Act, Crown Melbourne gave the AUSTRAC CEO SMRs with respect to Customer 11 on:

a. 11 March 2016;

b. 23 March 2016;

c. 11 April 2016 (2 SMRs); and

d. 28 May 2019.

Particulars

The SMRs described:

- losses noted for the key players under Customer 11's junket programs;

- suspicious transfers between Customer 11 and other junket operators; and
- suspicious telegraphic transfers to and from third parties.

1006. On each occasion that Crown Melbourne formed a suspicion with respect to Customer 11 for the purposes of s41 of the Act, it was required to apply its ECDD program to Customer 11.

Particulars

Rule 15.9(3) of the Rules.

1007. Crown Melbourne did not carry out appropriate risk-based ECDD measures with respect to Customer 11 on each occasion that Crown Melbourne formed a suspicion with respect to Customer 11 for the purposes of s41 of the Act.

a. There are no records of ECDD being conducted after giving the AUSTRAC CEO SMRs on 11 March 2016, 23 March 2016, 11 April 2016 (2 SMRs), and 28 May 2019: see paragraphs 664 and 685.

b. Appropriate risk-based steps were not taken to obtain or analyse information about Customer 11's source of wealth/funds, despite Crown Melbourne's knowledge of his connection to the Chinatown junket and ultimate beneficial owner Person 41: see paragraph 667.

c. Appropriate risk-based steps were not taken to analyse and monitor Customer 11's transactions – both past and future – including to understand their economic purpose: see paragraphs 590 and 666.

d. On each occasion prior to January 2021 that senior management considered whether to continue the business relationship with Customer 11, senior management failed to give adequate consideration to whether the ML/TF risks posed by Customer 11 was within Crown Melbourne's risk appetite: see paragraph 668ff.

Particulars

Rule 15.9(3), 15.10(1)(c), (d), (2), (5) and (6) of the Rules.

See particulars to paragraph 1004.

1008. Having formed a suspicion for the purposes of s41 of the Act, Crown Perth gave the AUSTRAC CEO SMRs with respect to Customer 11 on:

a. 31 March 2016;

b. 22 November 2016;

c. 20 January 2017; and

d. 3 November 2017.

Particulars

The SMRs described suspicious telegraphic transfers to and from third parties.

1009. On each occasion that Crown Perth formed a suspicion with respect to Customer 11 for the purposes of s41 of the Act, it was required to apply its ECDD program to Customer 11.

Particulars

Rule 15.9(3) of the Rules.

1010. Crown Perth did not carry out appropriate risk-based ECDD measures with respect to Customer 11 on each occasion that Crown Perth formed a suspicion with respect to Customer 11 for the purposes of s41 of the Act.

a. There are no records of ECDD being conducted after giving the AUSTRAC CEO an SMR on 31 March 2016, 22 November 2016, 20 January 2017 and 3 November 2017: see paragraphs 664 and 685.

b. Appropriate risk-based steps were not taken to obtain or analyse information about Customer 11's source of wealth/funds, despite Crown Perth's knowledge of his connection to the Chinatown junket and its ultimate beneficial owner, Person 41: see paragraph 667.

c. Appropriate risk-based steps were not taken to analyse and monitor Customer 11's transactions – both past and future – including to understand their economic purpose: see paragraphs 590 and 666.

d. On each occasion prior to January 2021 that senior management considered whether to continue the business relationship with Customer 11, senior management failed to give adequate consideration to whether the ML/TF risks posed by Customer 11 was within Crown Perth's risk appetite: see paragraph 668ff.

Particulars

Rule 15.9(3), 15.10(1)(c), (d), (2), (5) and (6) of the Rules.

See particulars to paragraph 1004.

1011. By reason of the matters pleaded from paragraphs 986 to 1010, on and from 1 March 2016, Crown Melbourne and Crown Perth:

a. did not monitor Customer 11 in relation to the provision of designated services, with a view to identifying, mitigating and managing the ML/TF risks reasonably faced; and

b. did not do so in accordance with rr15.5 and 15.9 of the Rules.

1012. By reason of the matters pleaded at paragraph 1011, Crown Melbourne contravened s36(1) of the Act on and from 1 March 2016 to 22 January 2021 with respect to Customer 11.

Particulars

Section 36(1) of the Act is a civil penalty provision: s36(2) of the Act.

1013. By reason of the matters pleaded at paragraph 1011, Crown Perth contravened s36(1) of the Act on and from 1 March 2016 to 16 February 2021 with respect to Customer 11.

Particulars

Section 36(1) of the Act is a civil penalty provision: s36(2) of the Act.

Customer 12

1014. Customer 12 was a customer of Crown Melbourne from 3 October 2015 to January 2021.

1015. From at least 3 October 2015, Crown Melbourne provided Customer 12 with designated services within the meaning of table 1 and table 3, s6 of the Act.

1016. From at least 21 April 2016, Customer 12 received designated services as a junket operator and junket player at Crown Melbourne.

Particulars to paragraphs 1015 and 1016

On 3 October 2015, Crown Melbourne opened a DAB account and safekeeping account (AUD/HKD) for Customer 12 under an initial PID, and made him a premium program player.

On 21 April 2016, Crown Melbourne entered into a NONEGPRA with Customer 12 to operate junkets at Crown Melbourne.

On the same day, Crown Melbourne opened additional DAB account and safekeeping accounts (AUD/HKD) for Customer 12 under his second PID.

Also on 21 April 2016, Crown Melbourne opened a credit facility for Customer 12 under his second PID. On 14 July 2017 Crown Melbourne closed this credit facility.

Between 22 April 2016 and 3 October 2016, Customer 12 facilitated at least 23 junket programs at Crown Melbourne as part of the Chinatown junket, with total turnover exceeding $253,059,235 in six months. During this period, Customer 12 had six junket representatives, including Person 23 and Person 40.

In 2019, Customer 12 received designated services as a junket player under Customer 4's junket programs.

On 20 January 2021, the Crown Resorts POI Committee considered Customer 12, who had come the Committee's attention through the ILGA inquiry, and agreed to issue a WOL in respect of Customer 12.

1017. Customer 12 was a customer of Crown Perth between 24 May 2016 and 29 January 2021.

1018. From 24 May 2016, Crown Perth provided Customer 12 with designated services within the meaning of table 1 and table 3, s6 of the Act.

1019. From at least 24 May 2016, Customer 12 received designated services as a junket operator at Crown Perth.

Particulars to paragraphs 1018 and 1019

By at least 22 April 2016, Crown Perth entered into a NONEGPRA with Customer 12.

On 26 May 2016, Crown Perth opened a DAB account and safekeeping account (AUD/HKD) for Customer 12 under a PID.

On the same day, Crown Perth a FAF for Customer 12 under two PIDs. On 11 October 2016, Crown Perth closed this credit facility.

Between 30 April 2016 and 21 August 2016, Customer 12 facilitated at least 15 junkets at Crown Perth as part of the Chinatown junket, with total turnover exceeding $1,155,125,183 in four months. During this period, Customer 12 had ten junket representatives, including Person 23 and Person 40.

On 29 January 2021, Crown Perth issued an NRL in respect of Customer 12 following the decision of the Crown Resorts POI Committee.

The ML/TF risks posed by Customer 12

1020. On and from mid-2016, designated services provided to Customer 12 posed higher ML/TF risks including because the provision of designated services to Customer 12 involved a combination of the following factors:

a. Customer 12 was a junket operator of the Chinatown junket;

b. by April 2016, as a result of Customer 12's connection to the Chinatown junket, Crown Melbourne and Crown Perth knew that Customer 12 was linked to Person 41 who was understood to be the ultimate beneficial owner of the Chinatown junket. This connection presented higher ML/TF risks for the reasons set out at paragraphs 968 and 969;

c. Customer 12 received high value financial services (table 1, s6) and gaming services (table 3, s6), through multiple junket programs: see paragraph 473ff;

d. Customer 12 was a junket operator who facilitated the provision of high value financial and gaming services (tables 1 and 3, s6) to key players (including foreign PEPs) on his junket programs: see paragraph 473ff;

e. between April 2016 and October 2016, Crown Melbourne recorded that the total turnover for junket programs operated by Customer 12 exceeded $253,059,235 in six months;

f. between April 2016 and August 2016, Crown Perth recorded that the total turnover for junket programs operated by Customer 12 exceeded $1,155,125,183 in four months;

g. designated services provided to Customer 12 lacked transparency as the services were provided through the channel of junket programs: see paragraph 477(e);

h. the table 3, s6, designated services provided to Customer 12 involved high turnover;

i. Customer 12 regularly made transfers to or received transfers from third parties, including third parties in respect of whom suspicions had been formed, and including to other junket operators;

j. designated services provided to Customer 12 involved large cross-border movements of funds: see paragraph 238(d);

k. Customer 12 made large and unusual requests for transfers to other Australian casinos, including, in August 2016, when Customer 12 arranged for $7,000,000 to be transferred from his Crown Perth DAB account to Customer 11's account at another Australian casino;

l. at various times, Customer 12 was provided with a significant amount of credit upon request, up to limits of AUD$140,000,000;

m. by reason of the matters set out at subparagraphs a. to l., and in light of his connections to the Chinatown junket, there were real risks that Customer 12's source of wealth/funds were not legitimate.

1021. At all times on and from mid-2016, Customer 12 should have been recognised by Crown Melbourne as a high risk customer by reason of the matters pleaded at paragraphs 1020, 1026, 1027, 1028 and 1030.

Particulars

Section 36(1)(a), (b) of the Act and Chapter 15 of the Rules.

1022. It was not until 20 January 2021 that Customer 12 was rated high risk by Crown Melbourne.

Particulars

On 11 occasions between 27 April 2016 and 4 October 2016, Crown Melbourne assessed Customer 12 as moderate risk.

See paragraph 481.

1023. At all times on and from mid-2016, Customer 12 should have been recognised by Crown Perth as a high risk customer by reason of the matters pleaded at paragraphs 1020, 1026, 1027, 1028 and 1033.

Particulars

Section 36(1)(a), (b) of the Act and Chapter 15 of the Rules

1024. It was not until 20 January 2021 that Customer 12 was rated high risk by Crown Perth.

Particulars

On 2 September 2016 and 21 February 2017, Crown Melbourne assessed Customer 12 as moderate risk.

See paragraph 481.

Monitoring of Customer 12's transactions

1025. At no time did Crown Melbourne appropriately monitor Customer 12's transactions on a risk-basis.

Particulars

Section 36(1)(a), (b) of the Act and rules 15.4 to 15.8 of the Rules..

Crown Melbourne was unable to monitor the ML/TF risks posed by transactions associated with Customer 12's junkets appropriately, including transactions by his junket representatives and key players on his junkets, because it did not make and keep appropriate records of designated services provided: see paragraphs 483ff.

Crown Melbourne did not apply appropriate risk-based transaction monitoring to designated services provided to Customer 12: see paragraphs 590ff and 629 to 642 (designated services) and 643 to 649 (transactions facilitated through junkets).

Ongoing customer due diligence

1026. On and from mid-2016, on multiple occasions, the provision of designated services to Customer 12 at Crown Melbourne and Crown Perth raised red flags reflective of higher ML/TF risks as a result of Customer 12's connection to Person 41 through the Chinatown junket.

Particulars

Section 36(1)(a), (b) of the Act and Chapter 15 of the Rules.

By 1 March 2016, Crown Melbourne and Crown Perth were aware that Person 41 was the ultimate beneficial owner and controller behind the Chinatown junket operations at Crown, including through Customer 12, and had financial interests in the business of the Chinatown junket: see particulars to paragraphs 968 and 969.

Links to the Chinatown junket

At the time that Customer 12 applied to be a junket operator, Crown Melbourne and Crown Perth were aware that Customer 12 was connected to the Chinatown junket and, as a result, also connected to Person 41.

Crown management understood that the Chinatown junket was replacing Customer 11 as the operator of the Chinatown junket at Crown with Customer 12, who was the brother of another individual associated with the Chinatown junket, Person 25, who provided guarantees for credit facilities provided by Crown to the Chinatown junket operators. Crown management also understood that this would involve transferring the Chinatown junket's credit arrangements with Crown, which were in the name of Customer 11 to Customer 12.

Between April 2016 and August 2016, Crown management regularly reapproved credit to Customer 12 to run junket programs at Crown Melbourne and Crown Perth, ranging from limits of AUD$60,000,000 and AUD$140,000,000 (HKD840,000,000), subject to a guarantee signed by Person 25 and Person 39.

2021

In February 2021, the Bergin Report found that prior to October 2016, Crown management was aware that Person 41 was a "financier" and "boss" of a number of 'Chinatown'-branded junkets run at both Crown Melbourne and Crown Perth, including by Customer 12. The Bergin Report described junket operators including Customer 12 as "front men" for the Chinatown junket and Person 41, and concluded that Crown did not have a real or proper understanding of these individuals to be satisfied they were of good repute.

1027. On and from mid-2016, on multiple occasions, the provision of designated services to Customer 12 at Crown Melbourne and Crown Perth raised red flags reflective of higher ML/TF risks arising from Customer 12's junket activity.

Particulars

See paragraphs 477.

Total junket activity at Crown Melbourne and Crown Perth

Between April 2016 and September 2016, the total turnover at Crown Melbourne for junket programs operated by Customer 12 was $253,059,235, with losses of $26,552,230.

Between April 2016 and September 2016, the total turnover at Crown Perth for junket programs operated by Customer 12 was $1,155,125,183, with losses of $23,668,511.

Junket activity (Crown Melbourne)

From April 2016 to June 2016, Crown Melbourne recorded gaming activity on junket programs operated by Customer 12 at Crown Melbourne as having turnover of $55,023,850 and losses of $2,458,750. Commissions of $1,536,719 were payable by Crown Melbourne to Customer 12.

From June 2016 to September 2016, Crown Melbourne recorded gaming activity on junket programs operated by Customer 12 at Crown Melbourne as having turnover of $198,035,385 and losses of $24,093,480. Commissions of $15,010,313 were payable by Crown Melbourne to Customer 12.

By 23 September 2016, key players on Customer 12's junkets had engaged in unusual activity. For example, a key player exchanged $500,000 in gaming chips for cash: SMR dated 23 September 2016.

Following the closure of the programs, five key players under Customer 12's junket programs were noted for high losses, totalling AUD$39,225,690 and HKD13,640,000. One of Customer 12's key players was a foreign PEP and individually noted as losing $24,016,500: SMR dated 31 August 2016.

Junket activity (Crown Perth)

From April 2016 to June 2016, Crown Perth recorded gaming activity on junket programs operated by Customer 12 at Crown Perth as having turnover of $18,980,000 and losses of $4,199,550. Commissions of $2,527,295 were payable by Crown Perth to Customer 12.

From July 2016 to September 2016, Crown Perth recorded gaming activity on junket programs operated by Customer 12 at Crown Perth as having turnover of $1,136,145,183 and losses of $19,468,961.

1028. On and from mid-2016, on multiple occasions, the provision of designated services to Customer 12 at Crown Melbourne and Crown Perth raised red flags reflective of higher ML/TF risks as a result of unusual transactions involving Customer 12 and his junket representatives.

Particulars

See paragraphs 420ff, 450, 451, 456ff and 491.

2016

On 26 April 2016, a telegraphic transfer of $100,000 was arranged from Customer 12's DAB account to a third party Australian company with the description 'Invoice': SMR dated 27 April 2016.

On 3 June 2016, a telegraphic transfer of $50,000 was deposited into Customer 12's DAB account from a third party based in Australia, Person 19, who was not noted as a key player under any of Customer 12's junkets: SMR dated 6 June 2016.

On 6 and 7 June 2016, two telegraphic transfers totalling $200,000 were deposited into Customer 12's DAB account from a third party based in Australia, who was not noted as a key player under any of Customer 12's junkets: SMR dated 7 June 2016.

On 28 July 2016, three telegraphic transfers were deposited into Customer 12's DAB account from the following third parties:

- $100,000 from a third party individual;
- $2,727,161 from a third party company; and
- $3,302,503 from a third party company: SMR dated 29 July 2016.

On 11 August 2016, Customer 12 arranged for $7,000,000 to be transferred from Customer 12's Crown Perth DAB account to Customer 11's account at another Australian casino. At the time, Crown Perth stated that both individuals were known to be junket operators but that it was unaware of the reason for the transfer. By March 2016, Customer 11 had ceased junket operations for the Chinatown junket at Crown Perth: SMR dated 17 August 2016.

On 4 October 2016, $520,000 was transferred from Customer 12's DAB account to the account of Customer 12's junket representative, Person 23. The junket representative then withdrew $500,000 in cash: SMR dated 5 October 2016.

2019

Between 5 September 2019 and 3 October 2019, Customer 12 attended Crown Melbourne and played under Customer 4's junket program. Customer 12's turnover was $154,275 with losses of $1,610.

1029. At no time did Crown Melbourne or Crown Perth undertake appropriate risk-based customer due diligence with respect to Customer 12 with a view to identifying, mitigating and managing the ML/TF risks posed by the provision of designated services on and from mid-2016.

a. At no time did Crown Melbourne or Crown Perth take appropriate steps to understand whether Customer 12's source of wealth/funds was legitimate, despite Crown Melbourne and Crown Perth's knowledge of his connection to the Chinatown junket and Person 41.

b. At no time did Crown Melbourne or Crown Perth take appropriate steps to identify or analyse the ML/TF risks of Customer 12's transactions or to consider whether they had a lawful purpose.

c. At no time did Crown Melbourne or Crown Perth give appropriate consideration to whether large and high risk transactions should be processed.

d. At no time did Crown Melbourne or Crown Perth take appropriate steps to consider Customer 12's relationship with Person 41 through the Chinatown junket and the ML/TF risks arising as a result of that association.

e. Prior to the decision to issue Customer 12 with a WOL/NRL in January 2021, there is no record of senior management considering whether continuing the business relationship with Customer 12 was within Crown Melbourne or Crown Perth's ML/TF risk appetite in light of the ML/TF risks posed by Customer 12.

Particulars

Section 36(1)(a) of the Act.

The due diligence steps taken by with respect to Customer 12 included:

Database searches

In April 2016 (following Customer 12's application to be the junket operator for Chinatown), June 2016 and December 2016, Crown Melbourne conducted a number of company and open source searches in respect of Customer 12.

Wealth reports

On 17 September 2016, Crown sought to obtain a wealth report on Customer 12, but Crown was advised that a report could not be compiled based on the information that Crown had provided.

Junket profile

By December 2016, the Credit control team had prepared a draft junket profile on Customer 12, which noted that no records had been returned for database searches or wealth report requests.

Senior management consideration

On 20 January 2021, the Crown Resorts POI Committee considered Customer 12, who had come to the Committee's attention through the ILGA inquiry. The POI Committee issued a withdrawal of license against Customer 12, which was applied by Crown Melbourne on 22 January 2021.

Prior to January 2021, none of these steps taken by Crown Melbourne and Crown Perth were proportionate to the ML/TF risks reasonably posed by Customer 12.

Enhanced customer due diligence

1030. Having formed a suspicion for the purposes of s41 of the Act, Crown Melbourne gave the AUSTRAC CEO an SMR with respect to Customer 12 on:

a. 27 April 2016;

b. 6 June 2016;

c. 7 June 2016;

d. 29 July 2016;

e. 1 August 2016 (2 SMRs);

f. 8 August 2016;

g. 31 August 2016;

h. 23 September 2016; and

i. 5 October 2016.

Particulars

The SMRs described:

- suspicious telegraphic transfers to and from third parties;
- high losses noted for the key players under Customer 12's junket program; and
- suspicious cash transactions involving Customer 12's junket representatives.

1031. On each occasion that Crown Melbourne formed a suspicion with respect to Customer 12 for the purposes of s41 of the Act, it was required to apply its ECDD program to Customer 12.

Particulars

Rule 15.9(3) of the Rules.

1032. Crown Melbourne did not carry out appropriate risk-based ECDD measures with respect to Customer 12 on each occasion that Crown Melbourne formed a suspicion with respect to Customer 12 for the purposes of s41 of the Act.

a. There are no records of ECDD being conducted after giving the AUSTRAC CEO SMRs on 27 April 2016, 6 June 2016, 7 June 2016, 29 July 2016, 1 August 2016 (2 SMRs), 8 August 2016, 31 August 2016, 23 September 2016 and 5 October 2016: see paragraphs 664 and 685.

b. Appropriate risk-based steps were not taken to obtain or analyse information about Customer 12's source of wealth/funds, despite Crown Melbourne's knowledge of his connection to the Chinatown junket and Person 41: see paragraph 667.

c. Appropriate risk-based steps were not taken to analyse and monitor Customer 12's transactions – both past and future – including to understand their economic purpose: see paragraphs 590 and 666.

d. Prior to the decision to issue Customer 12 with a WOL/NRL in January 2021, there is no record of senior management considering whether continuing the business relationship with Customer 12 was within Crown Melbourne's ML/TF risk appetite in light of the ML/TF risks posed by Customer 12: see paragraph 668ff.

Particulars

Rules 15.9(3), 15.10(1)(c), (d), (2), (5) and (6) of the Rules.

See particulars to paragraph 1029.

1033. Having formed a suspicion for the purposes of s41 of the Act, Crown Perth gave the AUSTRAC CEO an SMR with respect to Customer 12 on 17 August 2016.

Particulars

The SMR described a telegraphic transfer of $7,000,000 from Customer 12's Crown Perth DAB account to Customer 11's account at another Australian casino.

1034. On each occasion that Crown Perth formed a suspicion with respect to Customer 12 for the purposes of s41 of the Act, it was required to apply its ECDD program to Customer 12.

Particulars

Rule 15.9(3) of the Rules.

1035. Crown Perth did not carry out appropriate risk-based ECDD measures with respect to Customer 12 on each occasion that Crown Perth formed a suspicion with respect to Customer 12 for the purposes of s41 of the Act.

a. There are no records of ECDD being conducted after giving the AUSTRAC CEO an SMR on 17 August 2016: see paragraphs 664 and 685.

b. Appropriate risk-based steps were not taken to obtain or analyse information about Customer 12's source of wealth/funds, despite Crown Melbourne's knowledge of his connection to the Chinatown junket and Person 41: see paragraph 667.

c. Appropriate risk-based steps were not taken to analyse and monitor Customer 12's transactions – both past and future – including to understand their economic purpose: see paragraphs 590 and 666.

d. Prior to the decision to issue Customer 12 with a WOL/NRL in January 2021, there is no record of senior management considering whether continuing the business relationship with Customer 12 was within Crown Perth's ML/TF risk appetite in light of the ML/TF risks posed by Customer 12: see paragraph 668ff.

Particulars

Rule 15.9(3), 15.10(1)(c), (d), (2), (5) and (6) of the Rules.

See particulars to paragraph 1029.

1036. By reason of the matters pleaded from paragraphs 1014 to 1035, on and from mid-2016, Crown Melbourne and Crown Perth:

a. did not monitor Customer 12 in relation to the provision of designated services, with a view to identifying, mitigating and managing the ML/TF risks reasonably faced; and

b. did not do so in accordance with rr15.5 and 15.9 of the Rules.

1037. By reason of the matters pleaded at paragraph 1036, Crown Melbourne contravened s36(1) of the Act on and from mid-2016 to 22 January 2021 with respect to Customer 12.

Particulars

Section 36(1) of the Act is a civil penalty provision: s36(2) of the Act.

1038. By reason of the matters pleaded at paragraph 1036, Crown Perth contravened s36(1) of the Act on and from mid-2016 to 16 February 2021 with respect to Customer 12.

Particulars

Section 36(1) of the Act is a civil penalty provision: s36(2) of the Act.

Customer 13

1039. Customer 13 was a customer of Crown Melbourne from 7 February 2011 to 22 January 2021.

1040. From at least 7 February 2011, Crown Melbourne provided Customer 13 with designated services within the meaning of table 1 and table 3, s6 of the Act.

1041. From at least 7 February 2011, Customer 13 received designated services as a junket player and junket operator for the Chinatown junket at Crown Melbourne.

Particulars to paragraphs 1040 and 1041

On 7 February 2011, Crown Melbourne opened a DAB account and safekeeping account (AUD/HKD) for Customer 13 under his PID.

Between 2011 and 2016, Customer 13 received designated services as a junket player through junkets run by Chinatown junket operators, including Customer 10, Customer 11, Customer 12, and other operators including Person 4 and Person 39.

On 17 September 2016, Crown Melbourne entered into a NONEGPRA with Customer 13 to operate junkets at Crown Melbourne. Between 2 October 2016 and 24 October 2016, Customer 13 operated at least three junket programs at Crown Melbourne. During this period, Customer 13 had three junket representatives.

On 2 October 2016, Crown Melbourne opened a credit facility for Customer 13 under his PID. On 4 September 2019, Crown Melbourne closed this credit facility.

On 20 January 2021, the Crown Resorts POI Committee considered Customer 13, who had come the Committee's attention through the ILGA inquiry, and agreed to issue a WOL in respect of Customer 13.

On 22 January 2021, the WOL took effect at Crown Melbourne.

The ML/TF risks posed by Customer 13

1042. By 1 March 2016, higher ML/TF risks were indicated by the nature and purpose of Customer 13's business relationship with Crown Melbourne, the nature of the transactions he had been conducting, together with the suspicions Crown Melbourne itself had formed with respect to Customer 13.

Particulars

Section 36(1)(a), (b) of the Act and Chapter 15 of the Rules.

Customer 13 was a junket player, including on programs run by Chinatown junket operators. He received designated services through the channel of junket programs. This channel lacked transparency: see paragraph 477.

By 1 March 2016, Customer 13 suffered high losses as a key player under junket programs, including:

- By 27 March 2011, losses of $287,750 under a junket program run by Person 4, who ran the Hot Pot Junket until 2015 at Crown Melbourne: SMR dated 28 March 2011; and
- By 12 May 2013, losses of $1,020,750 under a junket program run by Person 39, who was associated with the Chinatown junket as a guarantor: SMR dated 13 May 2013.

Due diligence

By 1 March 2016, Crown Melbourne had not taken any due diligence steps taken with respect to Customer 13.

1043. As at 1 March 2016, Customer 13 should have been recognised by Crown Melbourne as a high risk customer for the reasons pleaded at paragraph 1042.

Particulars

Section 36(1)(a), (b) of the Act and Chapter 15 of the Rules.

1044. At all times on and from 1 March 2016, Customer 13 should have been recognised by Crown Melbourne as a high risk customer by reason of the matters pleaded at paragraphs 1042, 1046, 1048, 1049 and 1051.

Particulars

Section 36(1)(a), (b) of the Act and Chapter 15 of the Rules.

1045. It was not until 20 January 2021 that Customer 13 was rated high risk by Crown Melbourne.

Particulars

On four occasions between 28 March 2011 and 25 October 2016, Crown Melbourne assessed Customer 13 as moderate risk.

See paragraph 481.

1046. On and from 1 March 2016, designated services provided to Customer 13 posed higher ML/TF risks including because the provision of designated services to Customer 13 involved a combination of the following factors:

a. Customer 13 was a junket player, including on programs operated by Chinatown junket operators;

b. Customer 13 was a junket operator of the Chinatown junket;

c. by September 2016, as a result of Customer 13's connection to the Chinatown junket, Crown Melbourne knew that Customer 13 was linked to Person 41 who was understood to be the ultimate beneficial owner of the Chinatown junket. This connection presented higher ML/TF risks for the reasons set out at paragraphs 968 and 969;

d. Customer 13 received high value financial services (table 1, s6) and gaming services (table 3, s6), through multiple junket programs: see paragraph 473ff;

e. Customer 13 was a junket operator who facilitated the provision of high value financial and gaming services (tables 1 and 3, s6) to key players on his junket programs: see paragraph 473ff;

f. designated services provided to Customer 13 lacked transparency as the services were provided through the channel of junket programs: see paragraph 477(e);

g. designated services provided to Customer 13 involved large transfers to third parties: see paragraph 456ff;

h. the table 3, s6, designated services provided to Customer 13 involved high turnover;

i. at various times, Customer 13 was provided with a significant amount of credit up to limits of $140,000,000;

j. these transactions took place against the background of:

   i. Crown Melbourne being aware of Customer 13's connection to Person 4 who ran the Hot Pot Junket until 2015 at Crown Melbourne. In 2021, the Bergin Inquiry concluded that the Hot Pot Junket was linked to a prominent organised crime group; and

   ii. two SMRs being given to the AUSTRAC CEO by 1 March 2016;

k. by reason of the matters pleaded at subparagraphs a. to j. above, and in light of his connections to the Chinatown junket, there were real risks that Customer 13's source of wealth/funds were not legitimate.

Monitoring of Customer 13's transactions

1047. At no time did Crown Melbourne appropriately monitor Customer 13's transactions on a risk-basis.

Particulars

Section 36(1)(a), (b) of the Act and rules 15.4 to 15.8 of the Rules..

Crown Melbourne was unable to monitor the ML/TF risks posed by the transactions associated with Customer 13's junkets appropriately, including transactions by his junket representatives and key players on his junkets, because it did not make and keep appropriate records of designated services provided: see paragraphs 483ff.

Crown Melbourne did not apply appropriate risk-based transaction monitoring to designated services provided to Customer 13: see paragraphs 590ff and 629 to 642 (designated services) and 643 to 649 (transactions facilitated through junkets).

Ongoing customer due diligence

1048. On and from September 2016, on multiple occasions, the provision of designated services to Customer 13 at Crown Melbourne raised red flags reflective of higher ML/TF risks as a result of Customer 13's connection to Person 41 through the Chinatown junket.

Particulars

Section 36(1)(a), (b) of the Act and Chapter 15 of the Rules.

By 1 March 2016, Crown Melbourne and Crown Perth were aware that Person 41 was the ultimate beneficial owner and controller behind the Chinatown junket operations at Crown, including through Customer 13, and had financial interests in the business of the Chinatown junket.

See particulars to paragraphs 968 and 969.

Links to Chinatown

At the time that Customer 13 applied to be a junket operator, Crown management understood that Customer 13 was replacing Customer 12 as the operator of the Chinatown junket. Crown management also understood that this would involve transferring the Chinatown junket's credit arrangements with Crown, which were in the name of Customer 12 to Customer 13.

February 2021 – Bergin Report

The Bergin Report found that prior to October 2016, Crown management was aware that Person 41 was a "financier" and "boss" of a number of 'Chinatown'-branded junkets run at both Crown Melbourne and Crown Perth, including by Customer 13. The Bergin Report described junket operators including Customer 13 as "front men" for the Chinatown junket and Person 41, and concluded that Crown did not have a real or proper understanding of these individuals to be satisfied they were of good repute.

1049. On and from 1 March 2016, on multiple occasions, the provision of designated services to Customer 13 at Crown Melbourne raised red flags reflective of higher ML/TF risks.

Particulars

See paragraphs 456ff and 477.

Junket activity

On 2 October 2016, Crown management opened a credit facility for Customer 13, and approved a credit limit of AUD$140,000,000, subject to obtaining a guarantee from an individual associated with the Chinatown junket, Person 25 (the brother of Customer 12).

In October 2016, Customer 13 operated three junket programs at Crown Melbourne. Crown Melbourne recorded that the combined turnover for the programs was AUD$48,142,950 and HKD46,164,375. Commissions of AUD$279,793 and HKD234,165 were payable by Crown Melbourne to Customer 13.

Following the closure of the programs, two key players under Customer 13's junket were noted as having lost a combined total of $1,003,675: SMR dated 25 October 2016.

On 21 October 2016, Customer 13 arranged for a telegraphic transfer of $200,000 from his Crown Melbourne DAB account to a third party: SMR dated 24 October 2016.

1050. At no time did Crown Melbourne undertake appropriate risk-based customer due diligence with respect to Customer 13 with a view to identifying, mitigating and managing the ML/TF risks posed by the provision of designated services on and from 1 March 2016.

a. At no time did Crown Melbourne take appropriate steps to understand whether Customer 13's source of wealth/funds was legitimate, despite Crown Melbourne's knowledge of his connection to the Chinatown junket and Person 41.

b. At no time did Crown Melbourne take appropriate steps to identify or analyse the ML/TF risks of Customer 13's transactions or to consider whether they had a lawful purpose.

c. At no time did Crown Melbourne give appropriate consideration to whether large and high risk transactions should be processed.

d. At no time did Crown Melbourne take appropriate steps to consider Customer 13's relationship with Person 41 through the Chinatown junket and the ML/TF risks arising as a result of that association.

e. Prior to the decision to issue Customer 13 with a WOL/NRL in January 2021, there is no record of senior management considering whether continuing the business relationship with Customer 13 was within Crown Melbourne or Crown Perth's ML/TF risk appetite in light of the ML/TF risks posed by Customer 13.

Particulars

Section 36(1)(a) of the Act.

The due diligence steps taken with respect to Customer 13 included:

Database searches

Following receipt of Customer 13's application to be a junket operator and for a credit facility to run the junkets, on 26 September 2016, the Credit control team conducted a risk intelligence search. On the same day, Credit control received information from an overseas Crown employee that Customer 13 was a chairperson of an overseas company with a diversified portfolio in real estate, footwear and financial advisory.

Between 2016 and 2019, no further due diligence steps were taken.

Senior management consideration

On 20 January 2021, the Crown Resorts POI Committee considered Customer 13, who had come to the Committee's attention through the ILGA inquiry, and issued a withdrawal of license against Customer 13, that took effect at Crown Melbourne on 22 January 2021.

Prior to January 2021, none of these steps were proportionate to the ML/TF risks reasonably posed by Customer 13.

Enhanced customer due diligence

1051. Having formed a suspicion for the purposes of s41 of the Act, Crown Melbourne gave the AUSTRAC CEO SMRs with respect to Customer 13 on:

a. 24 October 2016; and

b. 25 October 2016.

Particulars

The SMRs described:

- losses noted for the key players under Customer 13's junket programs; and
- suspicious telegraphic transfers to and from third parties.

1052. On each occasion that Crown Melbourne formed a suspicion with respect to Customer 13 for the purposes of s41 of the Act, it was required to apply its ECDD program to Customer 13.

Particulars

Rule 15.9(3) of the Rules.

1053. Crown Melbourne did not carry out appropriate risk-based ECDD measures with respect to Customer 13 on each occasion that Crown Melbourne formed a suspicion with respect to Customer 13 for the purposes of s41 of the Act.

a. There are no records of ECDD being conducted after giving the AUSTRAC CEO SMRs on 24 October 2016 and 25 October 2016: see paragraphs 664 and 685.

b. Appropriate risk-based steps were not taken to obtain or analyse information about Customer 13's source of wealth/funds, despite Crown Melbourne's knowledge of his connection to the Chinatown junket and its ultimate beneficial owner, Person 41: see paragraph 667.

c. Appropriate risk-based steps were not taken to analyse and monitor Customer 13's transactions – both past and future – including to understand their economic purpose: see paragraphs 590 and 666.

d. Prior to the decision to issue Customer 13 with a WOL/NRL in January 2021, there is no record of senior management considering whether continuing the business relationship with Customer 13 was within Crown Melbourne's ML/TF risk appetite in light of the ML/TF risks posed by Customer 13: see paragraph 668ff.

Particulars

Rule 15.9(3), 15.10(1)(c), (d), (2), (5) and (6) of the Rules.

See particulars to paragraph 1050.

1054. By reason of the matters pleaded from paragraphs 1039 to 1053, on and from 1 March 2016, Crown Melbourne:

a. did not monitor Customer 13 in relation to the provision of designated services, with a view to identifying, mitigating and managing the ML/TF risks reasonably faced; and

b. did not do so in accordance with rr15.5 and 15.9 of the Rules.

1055. By reason of the matters pleaded at paragraph 1054, Crown Melbourne contravened s36(1) of the Act on and from 1 March 2016 to 22 January 2021 with respect to Customer 13.

Particulars

Section 36(1) of the Act is a civil penalty provision: s36(2) of the Act.

Customer 14

1056. Customer 14 was a customer of Crown Melbourne from 25 September 2017 to 22 January 2021.

1057. From at least 25 September 2017, Crown Melbourne provided Customer 14 with designated services within the meaning of table 1 and table 3, s6 of the Act.

1058. From at least 25 September 2017, Customer 14 received and facilitated designated services as a junket player and junket operator at Crown Melbourne.

Particulars to paragraphs 1057 and 1058

On 6 September 2017, Crown Melbourne entered into a NONEGPRA with Customer 14 to operate junkets at Crown Melbourne.

Between 30 September 2017 and 29 February 2020, Customer 14 facilitated at least 48 junkets at Crown Melbourne as part of the Chinatown junket. During this period, Customer 14 had 18 junket representatives, including Person 23 and Person 40.

On 25 September 2017, Crown Melbourne opened a DAB account and safekeeping account (AUD) Customer 14 under his initial PID.

On 27 September 2017, Crown Melbourne opened three further DAB accounts (AUD/HKD) for Customer 14, under a second, third and fourth PID.

On 20 January 2021, the Crown Resorts POI Committee considered Customer 14, who had come the Committee's attention through the ILGA inquiry, and agreed to issue a WOL in respect of Customer 14.

On 22 January 2021, the WOL took effect at Crown Melbourne.

The ML/TF risks posed by Customer 14

1059. On and from September 2017, designated services provided to Customer 14 posed higher ML/TF risks including because the provision of designated services to Customer 14 involved a combination of the following factors:

a. Customer 14 was a junket operator of the Chinatown junket;

b. by September 2017, Crown Melbourne should have known that Customer 14 was connected the Chinatown junket, and as a result linked to Person 41 who was understood to be the ultimate beneficial owner of the Chinatown junket. This connection presented higher ML/TF risks for the reasons set out at paragraphs 968 and 969:

   i. Customer 14's junket representatives also worked on junket programs run by other Chinatown junket operators, including Customer 10, Customer 11, Customer 12 and Customer 13;

ii. in March 2018, Customer 14 sent $360,000 to an Australian company known to be linked to Person 41;

iii. in May 2019, a former Chinatown junket operator Customer 11 worked as a junket representative for Customer 14;

iv. in February 2021, the Bergin Report concluded that it was clear to Crown that the Chinatown junket operators were linked to Person 41;

c. Customer 14 received high value financial services (table 1, s6) and gaming services (table 3, s6), through multiple junket programs: see paragraph 473ff;

d. Customer 14 was a junket operator who facilitated the provision of high value financial and gaming services (tables 1 and 3, s6) to key players on his junket programs: see paragraph 473ff;

e. designated services provided to Customer 14 lacked transparency as the services were provided through the channel of junket programs: see paragraph 477(e);

f. by no later than 2 August 2019, the total turnover at Crown Melbourne for junket programs operated by Customer 14 had exceeded $544,226,131;

g. Customer 14 and persons associated with his junket, transacted using large amounts of cash and cash that appeared suspicious: see paragraphs 450, 451, 452 and 491;

h. Customer 14 transacted in large values on his DAB account;

i. designated services provided to Customer 14 involved large transfers to third parties: see paragraph 456ff;

j. the table 3, s6, designated services provided to Customer 14 involved high turnover;

k. Customer 14's junket representatives engaged in other transactions indicative of ML/TF typologies and vulnerabilities, including attempting to cash-in large value chips with no evidence of play: see paragraph 24; and

l. by reason of the matters pleaded at subparagraphs a. to k. above, and in light of his connections to the Chinatown junket, there were real risks that Customer 14's source of wealth and source of funds were not legitimate.

1060. At all times on and from September 2017, Customer 14 should have been recognised by Crown Melbourne as a high risk customer by reason of the matters pleaded at paragraphs 1059, 1063, 1064, 1065 and 1067.

Particulars

Section 36(1)(a), (b) of the Act and Chapter 15 of the Rules.

1061. It was not until 20 January 2021 that Customer 14 was rated high risk by Crown Melbourne.

Particulars

On 11 occasions between 6 December 2017 and 29 January 2019, Crown Melbourne assessed Customer 14 as moderate risk.

See paragraph 481.

Monitoring of Customer 14's transactions

1062. At no time did Crown Melbourne appropriately monitor Customer 14's transactions on a risk-basis.

Particulars

Section 36(1)(a), (b) of the Act and rules 15.4 to 15.8 of the Rules..

Crown Melbourne was unable to monitor the ML/TF risks posed by the transactions associated with Customer 14's junkets appropriately, including transactions by his junket representatives and key players on his junkets, because it did not make and keep appropriate records of designated services provided to junket players: see paragraphs 483ff.

Crown Melbourne did not apply appropriate risk-based transaction monitoring to designated services provided to Customer 14: see paragraphs 590ff and 629 to 642 (designated services) and 643 to 649 (transactions facilitated through junkets).

Ongoing customer due diligence

1063. On and from September 2017, on multiple occasions, the provision of designated services to Customer 14 at Crown Melbourne raised red flags reflective of higher ML/TF risks as a result of Customer 14's connection to Person 41 through the Chinatown junket.

Particulars

Section 36(1)(a), (b) of the Act and Chapter 15 of the Rules.

By 1 March 2016, Crown Melbourne was aware that Person 41 was the ultimate beneficial owner and controller behind the Chinatown junket operations at Crown, including through Customer 14, and had financial interests in the business of the Chinatown junket.

See particulars to paragraphs 968 and 969.

Customer 14's links to the Chinatown junket

From September 2017 to February 2020, Customer 14's junket representatives included Person 23 and Person 40. These individuals also worked on junket programs run by other Chinatown junket operators, including Customer 10, Customer 11, and Customer 12.

In March 2018, Customer 14 sent $360,000 from his Crown Melbourne DAB account to an Australian company known to be linked to Person 41.

In 2019, Customer 11 was a junket representative for Customer 14's junket at Crown Melbourne.

2021

In February 2021, the Bergin Report found that prior to October 2016, Crown management was aware that Person 41 was a "financier" and "boss" of a number of 'Chinatown'-branded junkets run at both Crown Melbourne and Crown Perth, including by Customer 14. The Bergin

Report described junket operators including Customer 14 as "front men" for the Chinatown junket and Person 41, and concluded that Crown did not have a real or proper understanding of these individuals to be satisfied they were of good repute.

1064. On and from 2017, on multiple occasions, the provision of designated services to Customer 14 at Crown Melbourne raised red flags reflective of higher ML/TF risks arising from Customer 14's junket activity.

Particulars

See paragraph 477.

Total junket activity at Crown Melbourne

By 2 August 2019, the total turnover for junket programs operated by Customer 14 at Crown Melbourne was $544,226,131, with overall losses of $18,298,683. In total, commissions of $7,567,082 were payable by Crown Melbourne to Customer 14.

Junket activity in 2017

In 2017, Crown Melbourne was aware of the high losses noted for the key players under Customer 14's junket program, giving the AUSTRAC CEO an SMR that described losses by one key player under Customer 14's junket totalling HKD19,990,500: SMR dated 6 December 2017.

Junket activity in 2018

During the 2018 financial year, Customer 14's turnover at Crown Melbourne was $394,261,004, with losses of $15,304,347. Commissions of $6,199,131 were payable by Crown Melbourne to Customer 14.

Junket activity in 2019

During the 2019 financial year, Customer 14's junket turnover at Crown Melbourne was $144,445,677, with losses of $3,315,636. Commissions of $1,323,795 were payable by Crown Melbourne to Customer 14.

1065. On and from 2017, on multiple occasions, the provision of designated services to Customer 14 at Crown Melbourne raised red flags reflective of higher ML/TF risks as a result of unusual transactions involving Customer 14 and his junket representatives.

Particulars

See paragraphs 450,451, 456ff and 491.

Unusual transactions in 2017

Between 27 July 2017 and 1 August 2017, ten large telegraphic transfers totalling HKD52,160,000 from third parties based overseas were deposited into the DAB account of another junket operator at Crown. On 10 October 2017, Crown Melbourne was asked to deposit the funds into the DAB account of Customer 14 at another Australian

casino, but was subsequently advised that the transfer was not to proceed: SMR dated 11 October 2017.

Unusual transactions in 2018

On 2 January 2018, Customer 14's junket representative bought into a junket cash program with front money from Customer 14's safekeeping account, then immediately cashed out $86,500 after buy-in, advising the Cage that there was no intention of gaming under the program: SMR dated 3 January 2018.

On 18 February 2018, Customer 14's junket representative, Person 27, withdrew $2,000,000 in cash from Customer 14's DAB account: SMR dated 19 February 2018.

On 22 February 2018, Customer 14's junket representative Person 40 presented $500,000 in cash with instructions to deposit the cash into Customer 14's safekeeping account: SMR dated 23 February 2018.

On 2 March 2018, a telegraphic transfer of $360,000 was arranged from Customer 14's DAB account to a third party company known to be associated with Person 41: SMR dated 2 March 2018.

On 13 June 2018, $500,000 was transferred from Customer 14's DAB account to a third party's Crown DAB account, who was not a key player on Customer 14's junket: SMR dated 14 June 2018.

On 4 July 2018, Customer 14's junket representative, Person 27, withdrew $450,000 in cash from Customer 14's DAB account: SMR dated 5 July 2018.

On 15 August 2018, Customer 14 received a telegraphic transfer of $100,000 from a third party who was not a key player on Customer 14's junket: SMR dated 16 August 2018.

On 16 August 2018, Customer 14 received a second telegraphic transfer of $100,000 from a third party who was not a key player on Customer 14's junket: SMR dated 17 August 2018.

Unusual transactions in 2019

On 28 May 2019, Customer 14's junket representative, Person 27, transferred $100,000 from his bank account to his Crown DAB account, then exchanged the funds for gaming chips (3x $25,000; 4x $5,000). Customer 14's second junket representative, Customer 11, then presented gaming chips at the Cage in the same breakdown and requested to exchange the chips for cash. When questioned about the provenance of the gaming chips, Customer 11 said that they belonged to Person 2, a key player on Customer 14's junket in January 2019. Crown declined to process the transaction as there was no evidence that Person 2 owned the chips and returned the chips to Customer 11: SMR dated 28 May 2019.

Around 13 June 2019 and 2 July 2019, Customer 11 acted as a junket representative for Customer 14's junket program.

On 28 July 2019, a telegraphic transfer of $700,000 from Customer 14's DAB account was sent to the Australian bank account owned by Person 40 (one of Customer 14's junket representatives): SMR dated 29 July 2019.

In December 2019, a key player, Person 2, was losing under Customer 14's junket program (approximately $480,000). On 23 December 2019, a telegraphic transfer of $400,000 was received from a third party: SMR dated 24 December 2019.

1066. At no time did Crown Melbourne undertake appropriate risk-based customer due diligence with respect to Customer 14 with a view to identifying, mitigating and managing the ML/TF risks posed by the provision of designated services on and from September 2017.

a. At no time did Crown Melbourne take appropriate steps to understand whether Customer 14's source of wealth/funds was legitimate, despite Crown Melbourne's awareness of his connection to Person 41.

b. At no time did Crown Melbourne take appropriate steps to identify or analyse the ML/TF risks of Customer 14's transactions or to consider whether they had a lawful purpose.

c. With the exception of the decision to refuse to exchange gaming chips for cash in May 2019, at no time did Crown Melbourne give appropriate consideration to whether large and high risk transactions should be processed.

d. Despite Crown Melbourne's awareness of Customer 14's connection to Person 41, at no time did Crown Melbourne take appropriate steps to consider Customer 14's relationship with Person 41 through the Chinatown junket and the ML/TF risks arising as a result of that association.

e. On each occasion prior to January 2021 that senior management considered whether to continue the business relationship with Customer 12, senior management failed to give adequate consideration to whether the ML/TF risks posed by Customer 12 were within Crown Melbourne's risk appetite.

Particulars

Section 36(1)(a) of the Act.

The due diligence steps taken with respect to Customer 14 included:

Database searches

In September 2017 (after receiving his application to be a junket operator at Crown Melbourne) and July 2019 the Credit control team conducted risk intelligence searches in respect of Customer 14.

Wealth reports

In September 2017 and September 2019, the Credit control team requested wealth reports on Customer 14. In September 2017, Crown was advised that a report could not be compiled based on the information that Crown had provided.

Junket profile

In September 2017, the Credit control team prepared a junket profile with respect to Customer 14 that set out information obtained from searches and wealth reports.

By September 2019, the Credit control team updated Customer 14's junket profile, and recommended that Crown continue to conduct business with Customer 14 but did not provide a basis for this decision.

Senior management consideration

On 5 September 2017, the Senior Vice President (International Business) sought approval from senior management for Customer 14 to commence junket operations. He noted that Customer 14 wished to operate cash junkets at Crown and that there were no adverse findings from due diligence. The Chief Executive Officer (Australian Resorts), the Chief Legal Officer and a Crown Resorts director approved the recommendation.

On 20 January 2021, the Crown Resorts POI Committee considered Customer 14, who had come to the Committee's attention through the ILGA inquiry. The POI Committee made the decision to stop doing business with Customer 14.

On 22 January 2021, Crown Melbourne issued a WOL in respect of Customer 14.

Prior to January 2021, none of the due diligence steps taken by Crown Melbourne were proportionate to the ML/TF risks reasonably posed by Customer 14.

Enhanced customer due diligence

1067. Having formed a suspicion for the purposes of s41 of the Act, Crown Melbourne gave the AUSTRAC CEO an SMR with respect to Customer 14 on:

a. 11 October 2017;

b. 6 December 2017;

c. 3 January 2018;

d. 19 February 2018;

e. 23 February 2018;

f. 2 March 2018;

g. 14 June 2018;

h. 5 July 2018;

i. 16 August 2018;

j. 17 August 2018;

k. 28 May 2019;

l. 29 July 2019; and

m. 24 December 2019.

Particulars

The SMRs described:

- losses noted for the key players under Customer 14's junket programs; and
- suspicious telegraphic transfers to and from third parties.

1068. On each occasion that Crown Melbourne formed a suspicion with respect to Customer 14 for the purposes of s41 of the Act, it was required to apply its ECDD program to Customer 14.

Particulars

Rule 15.9(3) of the Rules.

1069. Crown Melbourne did not carry out appropriate risk-based ECDD measures with respect to Customer 14 on each occasion that Crown Melbourne formed a suspicion with respect to Customer 14 for the purposes of s41 of the Act.

a. There are no records of ECDD being conducted after giving the AUSTRAC CEO SMRs between 11 October 2017 and 24 December 2019: see paragraphs 664 and 685.

b. Appropriate risk-based steps were not taken to obtain or analyse information about Customer 14's source of wealth/funds, despite Crown Melbourne's awareness of his connection to Person 41: see paragraph 667.

c. Appropriate risk-based steps were not taken to analyse and monitor Customer 14's transactions – both past and future – including to understand their economic purpose: see paragraphs 590 and 666.

d. On each occasion prior to January 2021 that senior management considered whether to continue the business relationship with Customer 12, senior management failed to give adequate consideration to whether the ML/TF risks posed by Customer 12 were within Crown Melbourne's risk appetite: see paragraph 668ff.

Particulars

Rule 15.9(3), 15.10(1)(c), (d), (2), (5) and (6) of the Rules.

See particulars to paragraph 1066.

1070. By reason of the matters pleaded from paragraphs 1056 to 1069, on and from September 2017 to 22 January 2021, Crown Melbourne:

a. did not monitor Customer 14 in relation to the provision of designated services, with a view to identifying, mitigating and managing the ML/TF risks reasonably faced; and

b. did not do so in accordance with rr15.5 and 15.9 of the Rules.

1071. By reason of the matters pleaded at paragraph 1070, Crown Melbourne contravened s36(1) of the Act on and from September 2017 to 22 January 2021 with respect to Customer 14.

Particulars

Section 36(1) of the Act is a civil penalty provision: s36(2) of the Act.

Customer 15

1072. Customer 15 has been a customer of Crown Melbourne since April 1996.

1073. From at least December 2006, Crown Melbourne provided Customer 15 with designated services within the meaning of table 1 and table 3, s6 of the Act.

1074. From at least 2008, Customer 15 received designated services as a junket operator at Crown Melbourne.

Particulars to paragraphs 1073 and 1074

Between 25 June 2016 and 27 October 2019, Customer 15 operated 21 junket programs at Crown Melbourne: 20 under one PID and one under a second PID. In that period, Customer 15 had 11 unique junket representatives.

On 26 April 1996, Crown Melbourne opened a DAB account and safekeeping account (AUD/HKD) for Customer 15, which remains open. On 25 July 2019 and 24 November 2019, Crown Melbourne opened two further DAB accounts and safekeeping accounts, which remain open.

On 30 April 1998, Crown Melbourne opened a credit facility (AUD/HKD) for Customer 15.

By August 2017, Customer 15 had a credit limit of $10,000,000.

By May 2018, Customer 15's junket had a cumulative turnover at Crown Melbourne of $2,713,000,000 with a loss of $27,100,000.

1075. Customer 15 has been a customer of Crown Perth since May 1996.

1076. From at least December 2006, Crown Melbourne provided Customer 15 with designated services within the meaning of table 1 and table 3, s6 of the Act.

1077. From at least January 2012, Customer 15 received designated services as a junket operator at Crown Perth.

Particulars to paragraphs 1076 and 1077

Between 17 August 2016 and 2 October 2019, Customer 15 operated nine junket programs at Crown Perth. In that period, Customer 15 had seven unique junket representatives.

On various occasions, Customer 15 was given at least six PIDs at Crown Perth.

On 9 May 1996, Crown Perth opened a DAB account and safekeeping account (AUD/HKD) for Customer 15, which remains open. On 22 July 2005 and 16 February 2013, Crown Perth opened two further DAB accounts and safekeeping accounts (AUD/HKD) for Customer 15.

On 9 May 1996, Crown Perth opened a FAF account (AUD/HKD) for Customer 15, which was closed on 23 November 2020. On 16

February 2013, Crown Perth opened a further FAF account (AUD/HKD) for Customer 15, which was closed on 23 February 2015.

By May 2018, Customer 15's junket had a cumulative turnover at Crown Perth of $860,000,000 with a loss of $10,900,000.

The ML/TF risks posed by Customer 15

1078. By 1 March 2016, higher ML/TF risks were indicated by the nature and purpose of Customer 15's business relationship with Crown Melbourne and Crown Perth, the nature of the transactions he had been conducting, together with the suspicions Crown Melbourne and Crown Perth itself had formed with respect to Customer 15.

Particulars

Section 36(1)(a), (b) of the Act and Chapter 15 of the Rules.

Customer 15 was a junket operator. He received designated services through the channel of junket programs. This channel lacked transparency: see paragraph 477.

Junket activity to 1 March 2016

In FY2015, gaming activity on junket programs run by Customer 15 at Crown Melbourne involved turnover of $40,709,424 with losses of $549,499.

By 1 March 2016, on several occasions, Customer 15 operated a junket with only one key player.

SMRs to 1 March 2016

By 1 March 2016, Crown Melbourne had given the AUSTRAC CEO 19 SMRs in relation to Customer 15 – on 31 March 2005, 24 January 2008, 16 July 2009, 24 July 2009, 19 April 2010, 7 November 2011, 15 December 2011, 3 January 2012, 23 May 2012, 25 February 2013, 15 July 2013, 10 November 2014, 2 January 2015, 16 July 2015, 29 December 2015, 6 January 2016, 11 January 2016, 8 February 2016 and 29 February 2016. The SMRs reported unusual transactions indicative of structuring, large and unusual cash transactions by key players in Customer 15's junket, significant losses by key players in Customer 15's junket, telegraphic transfers to third parties and the amount of cash key players in Customer 15's junket were prepared to carry.

By 1 March 2016, Crown Perth had given the AUSTRAC CEO one SMR in relation to Customer 15 on 9 January 2012. The SMR reported a request by Customer 15's junket program to transfer $550,200 at settlement to a third party who was not a key player in the junket. Crown Perth understood the third party to be a business associate of Customer 15.

Large and unusual transactions to 1 March 2016

Between 23 March 2005 and 29 March 2005, a total of $966,670 was deposited into Crown's bank account in favour of Customer 15. This

comprised up to 36 deposits per day at different Australian bank branches: SMR dated 31 March 2005. The deposits were indicative of the ML/TF typology of smurfing. No due diligence steps were taken in respect of these suspicious transactions.

On 15 August 2005, Customer 15 sent a telegraphic transfer of $1,500,000 to his Crown Perth DAB account for repayment of a debt.

On 31 January 2007, a key player in Customer 15's junket requested that a telegraphic transfer of $700,000 be sent to a foreign company account: SMR dated 16 July 2009.

On 15 July 2013, a junket representative of Customer 15's junket program deposited into his DAB account and then withdrew $800,000 in cash despite having no rated gaming activity: SMR dated 15 July 2013. The transaction was indicative of the ML/TF typology of quick turnover of funds (without betting).

On 25 November 2014, Customer 15 sent a telegraphic transfer of $2,930,000 to his Crown Melbourne DAB account for repayment of a debt.

On 5 January 2016, 5 February 2016 and 26 February 2016, third parties who were not key players on Customer 15's junket sent three large telegraphic transfers in a foreign currency to Customer 15's Crown Melbourne DAB account: SMRs dated 6 January 2016, 8 February 2016 and 29 February 2016.

Other suspicious activity to 1 March 2016

On 22 July 2009, Crown Melbourne received a law enforcement inquiry in respect of Customer 15.

In January 2016, Customer 15 utilised the City of Dreams deposit service: see paragraphs 332ff and 334ff. Customer 15 attempted to settle an outstanding debt at Crown Melbourne. City of Dreams gave to Crown Melbourne an FCR indicating that a large cash sum in a foreign currency had been collected.

On 5 February 2016 and 26 February 2016, the Cage at City of Dreams sent Crown Melbourne a FCR which identified that two third parties had deposited a large cash sum in a foreign currency to be credited to Customer 15 at Crown Melbourne.

Due diligence conducted to 1 March 2016

By 1 March 2016, the due diligence steps taken with respect to Customer 15 included obtaining a wealth report, company searches and risk intelligence searches.

1079. By 1 March 2016, Customer 15 should have been recognised by Crown Melbourne as a high risk customer for the reasons pleaded at paragraphs 1078.

1080. It was not until 5 April 2017 that Customer 15 was rated high risk by Crown Melbourne.

Particulars

On various occasions between 24 January 2008 and 21 July 2009, Customer 15 was assessed to be moderate risk by Crown Melbourne.

On various occasions between 22 July 2009, after receiving a law enforcement inquiry, and 13 December 2011 Customer 15 was assessed to be significant risk by Crown Melbourne.

On various occasions between 14 December 2011 and 15 November 2016, Customer 15 was assessed to be moderate risk by Crown Melbourne.

On various occasions between 16 November 2016, after receiving a further law enforcement inquiry, and 4 April 2017 Customer 15 was assessed to be significant risk by Crown Melbourne.

On 5 April 2017, after determining Customer 15 to be a foreign PEP, Crown Melbourne assessed Customer 15 to be high risk for the first time. Crown Melbourne assessed Customer 15 to be high risk on various occasions between 5 April 2017 and 28 October 2021.

See paragraph 481.

1081. At all times on and from 1 March 2016, Customer 15 should have been recognised by Crown Melbourne as a high risk customer by reason of the matters pleaded at paragraphs 1078, 1085, 1086, 1087, 1088, 1089, 1091 and 1095.

Particulars

Section 36(1)(a), (b) of the Act and Chapter 15 of the Rules.

1082. By August 2016, Customer 15 should have been recognised by Crown Perth as a high risk customer for the reasons pleaded at paragraphs 1078, 1085, 1086, 1087, 1088, 1092 and 1095.

1083. At no point was Customer 15 recognised by Crown Perth to be a high risk customer.

Particulars

On various occasions between 27 December 2011 and 17 December 2018, Crown Perth assessed Customer 15 to be low risk.

By 1 March 2016, Customer 15 had significant junket turnover and had been the subject of one SMR at Crown Perth. Customer 15 and his junket had been involved in transactions indicative of the ML/TF typology of smurfing at Crown Perth.

In August 2016, Customer 15's junket representative deposited $500,000 in cash into Customer 15's Crown Perth DAB account. The cash comprised a large volume of $100, $50, $10 and $5. Three of the $50 notes were determined to be counterfeit.

See paragraph 481.

1084. At all times on and from August 2016, Customer 15 should have been recognised by Crown Perth as a high risk customer by reason of the matters pleaded at paragraphs 1078, 1085, 1086, 1087, 1088, 1092 and 1095.

Particulars

Section 36(1)(a), (b) of the Act and Chapter 15 of the Rules.

1085. On and from 1 March 2016 designated services provided to Customer 15 posed higher ML/TF risks including because the provision of designated services to Customer 15 involved a combination of the following factors:

a. Customer 15 was a junket operator;

b. Customer 15 received high value financial (table 1, s6) and gaming services (table 3, s6);

c. Customer 15 was a junket operator who facilitated the provision of high value financial and gaming services (tables 1 and 3, s6) to many key players (including foreign PEPs) on his junket programs: see paragraph 473ff;

d. Customer 15 was a foreign PEP: see paragraphs 118 and 663;

e. by May 2018, Customer 15's junket had a cumulative turnover at Crown Melbourne of $2,713,000,000 with a loss of $27,100,000 and a cumulative turnover at Crown Perth of $860,000,000 with a loss of $10,900,000;

f. designated services provided to Customer 15 lacked transparency as the services were provided through the channel of junket programs: see paragraph 477(e);

g. Customer 15 and persons associated with his junket, transacted using large amounts of cash and cash that appeared suspicious, including large volumes of cash in small notes and counterfeit cash: see paragraphs 450, 451, 452 and 491;

h. designated services provided to Customer 15 involved large transfers to and from third parties, including to and from foreign remittance service providers and unknown third parties: see paragraph 456ff;

i. designated services provided to Customer 15 involved large cross-border movements of funds, including through a Southbank account: see paragraph 239;

j. at various times, Customer 15 was provided with significant amounts of credit upon request, up to limits of $10,000,000: see paragraphs 280ff and 487;

k. Customer 15 or his junket representatives engaged in other transactions indicative of ML/TF typologies and vulnerabilities, including cuckoo smurfing: see paragraph 24;

l. these transactions took place against the background of:

    i. law enforcement having expressed an interest in Customer 15 in July 2009;

    ii. 19 SMRs being given to the AUSTRAC CEO by Crown Melbourne and one SMR being given by Crown Perth by 1 March 2016;

    iii. in March 2005, up to 36 deposits per day at different Australian bank branches totalling $966,670 were made in favour of Customer 15. These transactions were indicative of the ML/TF typology of smurfing;

iv. In July 2013, a junket representative of Customer 15's junket program deposited and withdrew $800,000 in cash despite having no rated gaming activity. This transaction was indicative of the ML/TF typology of quick turnover of funds (without betting);

v. Customer 15 had received significant telegraphic transfers from third parties who were not key players in Customer 15's junket program;

vi. Customer 15 had transacted via the City of Dreams overseas deposit service: see paragraphs 332ff and 334ff; and

m. in 2016, Customer 15 was the subject of a further law enforcement inquiry;

n. by June 2016, Crown Melbourne was aware that a key player in Customer 15's junket was an alleged leading member of a criminal syndicate;

o. by reason of the matters set out at subparagraphs a. to n. above, there were real risks that Customer 15's source of wealth and source of funds were not legitimate.

Monitoring of Customer 15's transactions

1086. At no time did Crown Melbourne or Crown Perth appropriately monitor Customer 15's transactions on a risk-basis.

Particulars

Section 36(1)(a), (b) of the Act and rules 15.4 to 15.8 of the Rules.

Crown Melbourne and Crown Perth were unable to monitor the ML/TF risks posed by Customer 15's transactions appropriately because they did not make and keep appropriate records of designated services provided to junket operators: see paragraphs 483ff.

Crown Melbourne and Crown Perth were unable to monitor the ML/TF risks posed by transactions associated with Customer 15's junkets, including transactions by his junket representatives and key players on his junkets, because it did not make and keep appropriate records of designated services provided.

Crown Melbourne and Crown Perth did not apply appropriate risk-based transaction monitoring to designated services provided to Customer 15: see paragraphs 590ff, 629 to 642 and 643 to 649.

Had appropriate risk-based transaction monitoring been applied, large and suspicious transactions could have been identified earlier: see paragraphs 686 and 687.

In 2021, an independent auditor identified Customer 15 as responsive to an ML/TF 'risk area' as a result of Customer 15's activity as a junket operator. The independent auditor noted that junkets are high risk for casino ML/TF activity and therefore patrons identified as junket operators, including Customer 15, presented a higher ML/TF risk to Crown Melbourne and Crown Perth.

Between 12 July 2016 and 29 November 2016, Customer 15 received into his Crown Melbourne DAB account through a

Southbank account a total of $5,672,375. In 2020, an independent auditor identified these 33 transactions as indicative of the ML/TF typology of cuckoo smurfing:

- $1,299,890 from an international money changer;
- $1,179,832 from Company 7;
- $979,865 from another company account;
- $872,940 from Company 9;
- $599,908 from another company account;
- $419,955 from another company account;
- $200,000 from another company account; and
- $119,985 from a remittance service.

Ongoing customer due diligence

1087. On and from 1 March 2016, on multiple occasions, the provision of designated services to Customer 15 raised red flags reflective of higher ML/TF risks as a result of Customer 15's junket activity.

Particulars

See paragraph 477.

On various occasions, Customer 15 operated junket programs with only one key player. Customer 15 also operated junket programs with multiple key players.

On various occasions, Crown Melbourne formed suspicions with respect to high losses noted for key players in Customer 15's junket programs.

In FY2016, Customer 15's junket had a turnover at Crown Melbourne $120,289,506 with a loss of $10,436,610.

In FY2017 (to 2 June 2017), Customer 15's junket had a turnover at Crown Melbourne of $33,482,000 with a win of $213,050.

By May 2018, Customer 15's junket had a cumulative turnover at Crown Melbourne of $2,713,000,000 with a loss of $27,100,000. Customer 15's junket had a cumulative turnover at Crown Perth of $860,000,000 with a loss of $10,900,000.

Customer 15's junket players

On 29 June 2016, Crown Melbourne conducted risk intelligence searches for several key players in Customer 15's junket. In respect of one key player, a search returned that he was an alleged leading member of a criminal syndicate who allegedly managed and operated the syndicate's narcotics distribution, karaoke, nightclub and pirated DVD businesses. The key player was reportedly wanted by a foreign law enforcement agency. Open source information, which does not

appear to have come to Crown Melbourne's attention, further allege the key player's involvement in prostitution.

1088. On and from 1 March 2016, on multiple occasions, the provision of designated services to Customer 15 raised red flags reflective of higher ML/TF risks as a result of complex, unusually large transactions and unusual patterns of transactions involving Customer 15 which had no apparent economic or visible lawful purpose.

Particulars

See paragraphs 420ff, 450, 451, 456ff and 491.

On 18 August 2016, Customer 15's junket representative deposited $500,000 in cash into Customer 15's Crown Perth DAB account. The cash comprised 8,600 $100 notes, 450,000 $50 notes, 39,480 $10 notes and 70 $5 notes. Three of the $50 notes were determined to be counterfeit: SMR dated 18 August 2016.

On 9 September 2016, Customer 15 received a telegraphic transfer of $38,519 from a third party who was not a key player on Customer 15's junket program: SMR dated 12 September 2016.

On 17 December 2018, a Crown Perth customer deposited into his Crown Perth DAB account $69,500 in cash together with $23,500 in chips. The Crown Perth customer then directed $27,507 to Customer 15's Crown Perth DAB account as well as directing funds to another junket operator. The Crown Perth customer was not a key player under either junket program. Customer 15 then sent the $27,507 by telegraphic transfer to Crown Melbourne in his favour for repayment of a debt owed there. No further reason was given for the transfer: SMR dated 28 February 2019.

1089. From November 2016, the provision of designated services to Customer 15 raised red flags reflective of higher ML/TF risks as a result of a law enforcement inquiry in respect of Customer 15.

Particulars

On 16 November 2016, Crown Melbourne received a law enforcement inquiry in respect of Customer 15.

1090. At no time did Crown Melbourne or Crown Perth undertake appropriate risk-based customer due diligence with respect to Customer 15 with a view to identifying, mitigating and managing the ML/TF risks posed by the provision of designated services on and from 1 March 2016.

a. Although Crown Melbourne obtained reports and conducted searches which set out Customer 15's source of wealth/funds, at no time did Crown Melbourne or Crown Perth take appropriate steps to understand whether Customer 15's source of wealth/funds was legitimate.

b. At no time did Crown Melbourne or Crown Perth take appropriate steps to identify or analyse the ML/TF risks of Customer 15's transactions or to consider whether they had a lawful purpose.

c. At no time did Crown Melbourne give appropriate consideration to whether large and high risk transactions should be processed.

d. On each occasion that senior management considered whether to continue the business relationship with Customer 15, senior management failed to give adequate consideration to whether the ML/TF risks posed by Customer 15 were within Crown Melbourne or Crown Perth's risk appetite.

Particulars

Section 36(1)(a) of the Act.

Due diligence searches – wealth and risk intelligence reports

In October 2016, December 2016, April 2018, May 2018, May 2019 and June 2019, Crown Melbourne obtained wealth reports in respect of Customer 15. The May 2019 wealth report identified Customer 15's high estimated net worth.

In December 2016, March 2018, October 2018, January 2019 and May 2019, Crown Melbourne conducted risk intelligence searches in respect of Customer 15.

In January 2017, Crown Melbourne obtained a risk intelligence report that identified that Customer 15 was a foreign PEP by association.

In February 2019, Crown Aspinalls received a risk intelligence report in respect of Customer 15 which was relied on by Crown Melbourne and Crown Perth as part of its due diligence in respect of Customer 15. The report identified Customer 15's business interests and high net worth and that Customer 15 was a foreign PEP by association.

Other due diligence searches

Between October 2017 and August 2017, Crown Melbourne conducted company and land registry searches in respect of Customer 15.

By October 2021, Crown Melbourne had conducted open sources and media report searches in respect of Customer 15.

Senior management engagement

In February 2017, the VIP Operations Committee recommended that Crown continue to conduct business with Customer 15.

In August 2017, May 2018, October 2019, Crown prepared a junket profile relating to Customer 15's junket. The ultimate recommendation on each occasion was that Crown continue to conduct business with Customer 15. On each occasion, the profile did not set out Customer 15's ML/TF risk and the recommendation did not take appropriate consideration of Customer 15's ML/TF risk.

2021 Remediation Project

In October 2021, Crown Melbourne conducted a review in respect of Customer 15. The review identified that searches conducted by Crown regarding Customer 15's source of wealth.

No due diligence steps were taken in respect of the significant telegraphic transfers received by Customer 15 into his Crown Melbourne DAB account from several third party companies: see particulars to paragraph 1086.

None of these steps were proportionate to the ML/TF risks reasonably posed by Customer 15 on and from 1 March 2016.

Enhanced customer due diligence

1091. Having formed a suspicion for the purposes of s41 of the Act, Crown Melbourne gave the AUSTRAC CEO SMRs with respect to Customer 15 on:

a. 29 June 2016;

b. 12 September 2016;

c. 13 October 2017; and

d. 21 March 2018.

Particulars

The SMRs reported losses noted for key players in Customer 15's junket, risk intelligence searches conducted in respect of key players in Customer 15's junket programs, telegraphic transfers received into Customer 15's DAB account from third parties and the amount of cash key players in Customer 15's junket were prepared to carry.

1092. Having formed a suspicion for the purposes of s41 of the Act, Crown Perth gave the AUSTRAC CEO SMRs with respect to Customer 15 on:

a. 18 August 2016; and

b. 17 December 2018.

Particulars

The 18 August 2016 SMR reported the suspicious cash transaction involved three counterfeit notes: see particulars to paragraph 1088.

The 17 December 2018 SMR reported the suspicious transfer of funds involving another Crown Perth patron and another Crown Perth junket operator: see particulars to paragraph 1088.

1093. On each occasion that Crown Melbourne and Crown Perth formed a suspicion with respect to Customer 15 for the purposes of s41 of the Act, it was required to apply its ECDD program to Customer 15.

Particulars

Rule 15.9(3) of the Rules.

1094. Crown Melbourne and Crown Perth did not carry out appropriate risk-based ECDD measures with respect to Customer 15 on each occasion that they formed a suspicion with respect to Customer 15 for the purposes of s41 of the Act.

a. There are no records of ECDD being conducted by Crown Melbourne following the lodgement of SMRs on 12 September 2016, 13 October 2017 and 21 March 2018: see paragraphs 664 and 685.

b. There are no records of ECDD being conducted by Crown Perth following the lodgement of SMRs on 18 August 2016 and 17 December 2018: see paragraphs 664 and 685.

c. Appropriate risk-based steps were not taken to analyse and monitor Customer 15's transactions – both past and future – including to understand their economic purpose: see paragraph 590 and 666.

d. On each occasion that senior management considered whether to continue the business relationship with Customer 15, senior management failed to give adequate consideration to whether the ML/TF risks posed by Customer 15 were within Crown Melbourne or Crown Perth's risk appetite.

Particulars

Rules 15.9(3), 15.10(1)(c), (d), (2), (5) and (6) of the Rules.

Prior to lodging the SMR on 29 June 2016, Crown Melbourne conducted risk intelligence searches in respect of key players in Customer 15's junket.

See particulars to paragraph 1090.

1095. At all times from 1 March 2016, Customer 15 was a foreign PEP.

Particulars

Section 36(1)(a) of the Act

On 5 April 2017, Crown Melbourne identified Customer 15 to be a foreign PEP on the basis that a co-director of his business operations was the former chief police officer of several states in a foreign country.

However, in October 2021, Crown Melbourne identified in an SMR that Customer 15 did not meet the prescribed definition of a PEP: SMR dated 28 October 2021.

1096. At all times from 1 March 2016, Crown Melbourne and Crown Perth was required to apply its ECDD program to Customer 15.

Particulars

Rules 15.9(2) and 15.11 of the Rules

See paragraphs 660, 663 and 666.

1097. Crown Melbourne and Crown Perth did not carry out appropriate risk-based ECDD measures with respect to Customer 15 on and from 1 March 2016 given his status as a foreign PEP. In particular:

a. Crown Melbourne and Crown Perth did not undertake a detailed analysis of Customer 15's KYC information or analyse the legitimacy of Customer 15's source of wealth/funds;

b. steps that were taken to seek and obtain senior management approval for continuing a business relationship with Customer 15 did not have adequate regard to the ML/TF risks posed by the customer; and

c. steps that were taken to seek and obtain senior management approval for Crown Melbourne and Crown Perth to continue to provide designated services to Customer 15 did not give adequate consideration to the ML/TF risks posed.

Particulars

Rules 15.10(2), 15.10(6), 15.11 of the Rules**.**

See paragraphs 1090 and 1094.

See paragraph 660, 663, 666, 667 and 668.

1098. On and from 5 April 2017, Crown Melbourne rated Customer 15 high risk.

Particulars

Crown Melbourne rated Customer 15 high risk on four occasions between 5 April 2017 and 21 October 2021: paragraph 1080.

1099. On each occasion that Crown Melbourne rated Customer 15 high risk, Crown Melbourne was required to apply its ECDD program to Customer 15.

Particulars

Rule 15.9(1) of the Rules.

See paragraph 661.

1100. Crown Melbourne did not carry out appropriate risk-based ECDD measures with respect to Customer 15 on each occasion that Crown Melbourne rated Customer 15 high risk.

Particulars

At no time did Crown Melbourne conduct ECDD following each occasion that it rated Customer 15 high risk: see paragraph 1090 and 1094.

See paragraphs 661, 666, 667 and 668.

1101. By reason of the matters pleaded from paragraphs 1072 to 1100, on and from 1 March 2016, Crown Melbourne and Crown Perth:

a. did not monitor Customer 15 in relation to the provision of designated services, with a view to identifying, mitigating and managing the ML/TF risks it reasonably faced; and

b. did not do so in accordance with rr 15.5 and 15.9 of the Rules.

1102. By reason of the matters pleaded at paragraph 1101, Crown Melbourne and Crown Perth contravened s36(1) of the Act on and from 1 March 2016 with respect to Customer 15.

Particulars

Section 36(1) of the Act is a civil penalty provision: s36(2) of the Act.

Customer 16

1103. Customer 16 has been a customer of Crown Melbourne since 2 August 2017.

1104. From at least 2 August 2017, Crown Melbourne provided Customer 16 with designated services within the meaning of table 1 and table 3, s6 of the Act.

1105. From at least 2 August 2017, Customer 16 received designated services as a junket operator at Crown Melbourne.

Particulars to paragraphs 1104 and 1105

On 29 April 2017, Crown Melbourne entered into a NONEGPRA with Customer 16 to operate junkets at Crown Melbourne. Between August 2017 and October 2019, Customer 16 facilitated at least nine junkets at Crown Melbourne for key players, including Customer 32.

On 14 August 2017, Crown Melbourne opened a DAB account and safekeeping account for Customer 16.

On 2 August 2017, Crown Melbourne approved a credit facility (AUD/HKD) for Customer 16. On 20 November 2020, Crown Melbourne closed this credit facility.

1106. Customer 16 has been a customer of Crown Perth since 2 August 2017.

1107. From at least 3 August 2017, Crown Perth provided Customer 16 with designated services within the meaning of table 1 and table 3, s6 of the Act.

1108. From at least 3 August 2017, Customer 16 received designated services as a junket operator at Crown Perth.

Particulars to paragraphs 1107 and 1108

On 29 April 2017, Crown Perth entered into a NONEGPRA with Customer 16 to operate junkets at Crown Perth. Between August 2017 and October 2019, Customer 16 facilitated at least 15 junkets at Crown Perth for key players, including Customer 32.

On 17 August 2017, Crown Perth opened a DAB account and safekeeping account for Customer 16.

On 3 August 2017, Crown Perth approved a credit facility (AUD/HKD) for Customer 16. On 20 November 2020, Crown Perth closed this credit facility.

The ML/TF risks posed by Customer 16

1109. At all times on and from August 2017, Customer 16 should have been recognised by Crown Melbourne as a high risk customer by reason of the matters pleaded at paragraphs 1112, 1113, 1114, 1115, 1116 and 1118.

Particulars

Section 36(1)(a), (b) of the Act and Chapter 15 of the Rules.

On various occasions between 22 May 2017 and 5 June 2019, Crown Melbourne assessed Customer 16 as moderate risk.

This was despite that Customer 16 was a junket operator closely associated with another junket operator, Person 1, in respect of whom Crown Melbourne had formed suspicions.

See paragraph 481.

1110. At all times on and from August 2017, Customer 16 should have been recognised by Crown Perth as a high risk customer by reason of the matters pleaded at paragraphs 1112, 1113, 1114, 1115, 1116 and 1121.

Particulars

Section 36(1)(a), (b) of the Act and Chapter 15 of the Rules.

On 29 August 2017, Crown Perth assessed Customer 16 as low risk.

On 6 October 2017 and 2 January 2019, Crown Perth assessed Customer 16 as significant risk.

This was despite that Customer 16 was a junket operator closely associated with another junket operator, Person 1, in respect of whom Crown Perth had formed suspicions.

See paragraph 481.

1111. At no time was Customer 16 rated high risk by Crown Melbourne or Crown Perth.

1112. From August 2017, designated services provided to Customer 16 posed higher ML/TF risks including because the provision of designated services to Customer 16 involved a combination of the following factors:

a. Customer 16 received high value financial (table 1, s6) and gaming services (table 3, s6) provided through multiple junket programs: see paragraph 473ff;

b. Customer 16 was a junket operator who facilitated the provision of high value financial and gaming services (tables 1 and 3, s6) to key players (including Customer 32) on his junket programs: see paragraph 473ff;

c. Customer 16 was a junket operator;

d. by no later than January 2021, Crown Melbourne recorded that gaming activity on junket programs operated by Customer 16 at Crown Melbourne exceeded $148,000,000;

e. by no later than January 2021, Crown Perth recorded that gaming activity on junket programs operated by Customer 16 at Crown Perth exceeded $340,000,000;

f. Customer 16 was known at all times to be connected to other junket operators, including his deceased brother, Person 1, in respect of whom Crown Melbourne and Crown Perth had formed suspicions. Customer 16 took over junket operations from Person 1 in August 2017**;**

g. designated services provided to Customer 16 lacked transparency as the services were provided through the channel of junket programs: see paragraph 477(e);

h. the table 3, s6, designated services provided to Customer 16 involved high turnover;

i. designated services provided to Customer 16 involved large transfers to and from third parties, including to and from other junket operators, foreign remittance service providers

including the Company 10 deposit service and unknown third parties: see paragraphs 332ff, 359ff and 456ff;

j. designated services provided to Customer 16 involved large cross-border movements of funds, including through a Riverbank account: see paragraph 239;

k. large values were transferred to and from Customer 16's bank accounts and his DAB account, and to and from other customers' DAB accounts, involving the provision by Crown Melbourne of designated services within the meaning of items 31 and 32, table 1, s6 of the Act: see paragraphs 411ff and 492;

l. at various times, Customer 16 was provided with significant amounts of credit upon request, including a standing credit line with a limit of $3,000,000 which was reapproved on a regular basis until 2019: see paragraphs 280ff and 487;

m. Customer 16 received large transfers from other Australian casinos: 398ff and 407ff;

n. Customer 16 or his junket representatives engaged in other transactions indicative of ML/TF typologies and vulnerabilities, including offsetting (including with unrelated third parties): see paragraph 24;

o. by May 2017, Crown Melbourne and Crown Perth were aware that Customer 16's father was allegedly involved in illicit activities associated with junket operators, massage parlours and nightclubs until he was reportedly murdered in April 1994; and

p. by reason of the matters set out at subparagraphs a. to o. above, there were higher ML/TF risks associated with Customer 16's source of wealth/funds.

Monitoring of Customer 16's transactions

1113. At no time did Crown Melbourne or Crown Perth appropriately monitor Customer 16's transactions on a risk-basis.

Particulars

Section 36(1)(a), (b) of the Act and rules 15.4 to 15.8 of the Rules.

Crown Melbourne and Crown Perth were unable to monitor the ML/TF risks posed by Customer 16's transactions appropriately because they did not make and keep appropriate records of designated services provided to junket players or operators: see paragraphs 483ff.

Crown Melbourne and Crown Perth did not apply appropriate risk-based transaction monitoring to designated services provided to Customer 16: see paragraphs 590ff, 629 to 642 and 643 to 649.

Customer 16's transactions involved repeated transactions indicative of ML/TF typologies and vulnerabilities that were not detected prior to a 2020 and 2021 look-back. Had appropriate risk-based transaction monitoring been applied, these transactions could have been identified earlier: see paragraphs 686 and 687.

In 2020, an independent expert identified ten deposits into a Riverbank account totalling $2,244,477 for Customer 16's credit between September 2017 and December 2017, containing a

reference ‘purchasing good’. Seven deposits were from Person 10 and three deposits were from another third party.

Transactions involving Customer 16 were identified by an independent auditor in 2021 as involving the risk factor of third party transfers. Between 11 May 2020 and 13 May 2020, Customer 16 received two payments from third parties into a Crown Patron account totalling $499,940.

In 2021, an independent auditor identified Customer 16 as responsive to an ML/TF ‘risk area’ as a result of Customer 16’s activity as a junket operator. The independent auditor noted that junkets are high risk for casino ML/TF activity and therefore patrons identified as junket operators, including Customer 16, presented a higher ML/TF risk to Crown Melbourne and Crown Perth.

Ongoing customer due diligence

1114. On and from August 2017, the provision of designated services to Customer 16 by Crown Melbourne and Crown Perth raised red flags reflective of higher ML/TF risks due to Customer 16’s association with a junket operator, Person 1, in respect of whom Crown Melbourne and Crown Perth had formed suspicions.

Particulars

See paragraphs 24 and 477.

At the time Customer 16 applied to be a junket operator in April 2017, Crown Melbourne and Crown Perth were aware that Customer 16 was taking over the junket operations from his recently deceased brother, Person 1, who had operated junkets at Crown properties since 1995. Customer 16 had been involved in running his brother Person 1’s junket business since at least late 2016.

Crown Perth

By 30 January 2017, Person 1 had run approximately 353 junket programs at Crown Perth between 1995 and 2017. Crown Perth recorded that gaming activity on junket programs run by Person 1 at Crown Perth had involved a cumulative turnover of $5,164,583,903 with cumulative losses of $110,119,164. Commissions of $40,382,436 were payable by Crown Perth to Person 1.

Between 20 June 2007 and 27 June 2016, Crown Perth had given to the AUSTRAC CEO 63 SMRs which reported on transactions indicative of ML/TF typologies involving Person 1, his junket representatives and his junket players that had taken place during the junket programs.

24 SMRs related to transactions indicative of the ML/TF typology of refining, involving the exchange of smaller denomination notes for higher denomination notes.

12 SMRs related to transactions indicative of the ML/TF typology of cashing-in large value chips with no evidence of play.

One SMR related to transactions indicative of the ML/TF typology of structuring cash deposits, involving ten deposits of $9,000 and two deposits of $5,000, completed at bank branches in Sydney to a total of $100,000.

Seven SMRs related to large and suspicious cash deposits either deposited into Person 1's DAB account or used to purchase cash chips, not junket program chips.

Nine SMRs related to buy-in using bank cheques, which were exchanged for cash or cash chips.

Eight SMRs related to suspicious cash withdrawals in circumstances that did not correspond with recorded play under the junket programs.

Two SMRs related to telegraphic transfers of funds withdrawn from Person 1's Crown Perth DAB account to another junket operator at Crown Melbourne.

Crown Melbourne

By 3 February 2017, Person 1 had run approximately 132 junket programs at Crown Melbourne between 1995 and 2015. Gaming activity on junket programs run by Person 1 at Crown Melbourne had involved a cumulative turnover of $1,729,219,300 with cumulative losses of $27,712,110. Commissions of $13,811,679 were payable by Crown Melbourne to Person 1.

Between 31 December 2007 and 23 December 2012, Crown Melbourne had given to the AUSTRAC CEO nine SMRs with respect to Person 1. Six SMRs related to suspicions formed by Crown Melbourne regarding high losses noted for key players under Person 1's junkets. Two SMRs related to large telegraphic transfers from Person 1's Crown Melbourne DAB account to third parties totalling $1,787,000. The remaining SMR related to a suspicious cash deposit of $500,000.

1115. On and from August 2017, on multiple occasions, the provision of designated services to Customer 16 by Crown Melbourne and Crown Perth raised red flags reflective of higher ML/TF risks as a result of Customer 16's junket activity.

Particulars

See paragraph 477.

Total junket activity

Between August 2017 and January 2021, Crown Melbourne recorded that gaming activity on junket programs operated by Customer 16 at Crown Melbourne involved turnover of approximately $148,000,000 with losses of $7,900,000.

Between August 2017 and January 2021, Crown Perth recorded gaming activity on junket programs operated by Customer 16 at Crown Perth involved turnover of approximately $340,000,000 with losses of $100,000.

Junket activity (Crown Melbourne)

In December 2017, Customer 16 operated a junket program at Crown Melbourne. Crown Melbourne recorded that the turnover was $9,336,285, with commission payable to Customer 16 of $130,708. In December 2017, high losses were noted for four key players under Customer 16's junket program, totalling $1,501,540: SMR dated 13 December 2017.

In May 2018, Customer 16 operated a junket program at Crown Melbourne. Crown Melbourne recorded that the turnover was $19,743,000, with commission payable to Customer 16 of $276,402. At the close of the junket program in May 2018, high losses were noted for two key players under Customer 16's junket program, including Customer 32, totalling $2,295,400: SMR dated 9 May 2018.

In June 2018, Customer 16 operated a junket program at Crown Melbourne. Crown Melbourne recorded that the turnover was $3,326,000, with commission payable to Customer 16 of $53,216. At the close of the junket program in June 2018, high losses were noted for one key player under Customer 16's junket program, totalling $831,100: SMR dated 26 June 2018.

Between August 2017 and June 2018, Customer 16 ran at least four junket programs at Crown Melbourne. Crown Melbourne recorded that the cumulative turnover for those programs was $93,382,000 with cumulative losses of $4,458,635. Commissions of $747,056 were payable by Crown Melbourne to Customer 16.

In 2019, Customer 16 ran at least five junket programs at Crown Melbourne.

Junket activity (Crown Perth)

In 2017, Customer 16 ran at least five junket programs at Crown Perth, including at least four programs where Customer 32 was the key player.

In 2018, Customer 16 ran at least four junket programs at Crown Perth, including at least two programs where Customer 32 was the key player.

In 2019, Customer 16 ran at least six junket programs at Crown Perth.

Junket credit

Between 2017 and 2020, Crown management regularly reapproved Customer 16's junket credit facility, with limits between $1,000,000 and $3,000,000, as part of a monthly junket review.

1116. On and from August 2017, on multiple occasions, the provision of designated services to Customer 16 by Crown Melbourne and Crown Perth raised red flags reflective of higher ML/TF risks as a result of unusual transactions and patterns of transactions involving Customer 16 and foreign remittance service providers including the Company 10 deposit service.

Particulars

See paragraphs 332ff, 359ff, 420ff and 456ff.

Unusual transactions and patterns of transactions 2017

On 29 August 2017, Customer 16's junket representative withdrew $500,000 from Customer 16's Crown Perth DAB account and sent the funds by telegraphic transfer following the completion of a junket program. The funds were directed to a third party Australian company. Following inquiries, Crown Perth confirmed with Customer 16 that the funds ultimately belonged to him, but he had sold the funds to Company 10, a money changer operated by Person 56. At the same time that the funds were sold, Person 56 received a request from the Australian company to purchase $500,000. As such, Person 56 advised Customer 16 to transfer the funds from Customer 16's Australian bank account to the company who required them in order to purchase property in Australia. However, Customer 16's junket representative sent the funds directly to the Australian company from Customer 16's Crown Perth DAB account instead: SMR dated 12 September 2017.

On 28 November 2017, Crown Melbourne received a telegraphic transfer of $1,000,000 for the benefit of Customer 16 from the Company 10 deposit service through Person 56, which was to be used as front money. On 12 December 2017, Crown Melbourne recorded that the funds had been repurchased and recorded it as a credit in Customer 16's DAB account.

On 30 November 2017, Crown Melbourne received a telegraphic transfer of $21,771 for the benefit of Customer 16 from Crown Perth which was deposited into Customer 16's Crown Melbourne DAB account.

On 6 December 2017, Crown Melbourne received a telegraphic transfer of $50,000 from a third party, Person 10, which was deposited into Customer 16's Crown Melbourne DAB account.

On 21 December 2017, Crown Melbourne received a telegraphic transfer of $975,609 for the benefit of Customer 16 from Crown Perth. The funds were used to redeem Customer 16's credit marker.

On 28 December 2017, Crown Melbourne received a telegraphic transfer of $11,905 for the benefit of Customer 16 from Crown Perth. The funds were used to redeem Customer 16's credit marker.

Unusual transactions and patterns of transactions 2018

On 7 February 2018, Customer 16 received a $440,000 telegraphic transfer from his account at another Australian casino into his Crown Melbourne DAB account. The funds were immediately transferred from Customer 16's DAB account to Person 56's DAB account. Person 56 then requested that the $440,000, plus an additional $110,324, be transferred to another Crown patron's account: SMR dated 13 February 2018.

On 23 May 2018, Crown Melbourne received one telegraphic transfer of $800,000 for the benefit of Customer 16 from another Australian casino. The funds were used to redeem Customer 16's credit marker.

On 4 June 2018, Crown Melbourne received one telegraphic transfer of $388,404 for the benefit of Customer 16 from another Australian casino. The funds were deposited into Customer 16's Crown Melbourne DAB account.

On 9 June 2018, Crown Melbourne received two telegraphic transfers of $262,412 and $261,200 respectively for the benefit of Customer 16 from a third party, Person 34. On the same day, Crown Melbourne also received a third telegraphic transfer of $260,000 for the benefit of Customer 16 from another third party. The funds were used to redeem Customer 16's credit marker.

On 15 June 2018, Crown Melbourne received one telegraphic transfer of $1,000,000 for the benefit of Customer 16 from the Company 10 service through Person 56, which was to be used as front money. On 12 July 2018, the front money was returned by telegraphic transfer to Person 56.

On 30 June 2018, Crown Melbourne received one telegraphic transfer of $595,768 for the benefit of Customer 16 from Crown Perth, which was deposited into Customer 16's Crown Melbourne DAB account.

On 12 July 2018, Crown Melbourne received one telegraphic transfer of $249,270 for the benefit of Customer 16 from a third party. The funds were used to redeem Customer 16's credit marker.

Unusual transactions and patterns of transactions 2019

On 25 February 2019, Crown Melbourne received one telegraphic transfer of $244,817 for the benefit of Customer 16 from another Australian casino, which was deposited into Customer 16's Crown Melbourne DAB account.

On 22 February 2019, another junket operator withdrew $407,450 from her Crown Perth DAB account and transferred it to Customer 16's Crown Melbourne DAB account, at the instruction of her key player, because the key player and Customer 16 were 'friends.' The funds were used to redeem Customer 16's credit marker: SMR dated 26 March 2019.

1117. At no time did Crown Melbourne or Crown Perth undertake appropriate risk-based customer due diligence with respect to Customer 16 with a view to identifying, mitigating and managing the ML/TF risks posed by the provision of designated services on and from August 2017.

a. At no time did Crown Melbourne or Crown Perth take appropriate steps to understand whether Customer 16's source of wealth/funds was legitimate.

b. At no time did Crown Melbourne or Crown Perth take appropriate steps to identify or analyse the ML/TF risks of Customer 16's transactions or to consider whether they had a lawful purpose.

c. At no time did Crown Melbourne or Crown Perth give appropriate consideration to whether large and high risk transactions should be processed.

d. On each occasion that senior management considered whether to continue the business relationship with Customer 16, senior management failed to give adequate consideration to whether the ML/TF risks posed by Customer 16 were within Crown Melbourne or Crown Perth's risk appetite.

Particulars

Section 36(1)(a) of the Act.

The due diligence steps taken with respect to Customer 16 included:

Application for credit as a junket operator

In early May 2017, the Credit control team performed Australian company, risk intelligence, property and open source searches in respect of Customer 16.

On 15 May 2017 and 4 August 2017, Crown obtained wealth reports in respect of Customer 16. One of the wealth reports indicated that Customer 16's father owned massage parlours and nightclubs and ran junkets in various countries including Australia, was allegedly involved in illicit activities and was reportedly murdered in 1994.

The information used in the searches and wealth reports were used to prepare a junket profile for the purpose of assessing Customer 16's creditworthiness. By 8 August 2017, the profile:

- noted that the junket was previously in the name of Customer 16's brother, Person 1, who was deceased;
- set out gaming activity under Person 1's junket;
- set out Customer 16's junket operator credit lines at other casinos, including at another Australian casino; and
- noted that a Crown employee estimated Customer 16's wealth to be very high.

Further Australian company, property, media, and risk intelligence searches were conducted in 2018 and 2019.

Further wealth reports were obtained on 5 April 2018, 12 April 2018, 19 March 2019 and 28 March 2019, 10 November 2020. The report dated 10 November 2020 alleged that Customer 16's father was considered the 'godfather' of the gambling underworld and entertainment centres in a foreign country and was killed in April 1994.

The junket profile was updated on 9 May 2018, and 11 November 2019 with information obtained from the searches and wealth reports (but not the adverse information regarding Customer 16's father), and included a recommendation that Crown continue to conduct business with Customer 16. The recommendation was amended on 5

December 2019 to continue business with Customer 16 subject to obtaining a police clearance.

In March 2021, the junket profile was updated to include adverse information on Customer 16's father, as well as details of the risk intelligence and media searches performed in relation to Customer 16's name and known aliases, as well as his associates.

Senior management engagement

On 11 May 2017, Customer 16's junket operator application to take over Person 1's junket operations at Crown Melbourne and Crown Perth was considered by the VIP Operations meeting attended by a Crown Resorts director, the Chief Executive Officer (Australian Resorts), the Senior Vice President (International Business), the Group General Manager (International Business Operations) and the Chief Legal Officer (Australian Resorts). The committee resolved to allow Customer 16 to commence business with credit of $1,000,000.

On 5 June 2019, the Group General Manager (AML) requested records of third party transfers received for Customer 16 from January 2017 onwards. The CTRM responded noting that there were 18 telegraphic transfers, including from foreign remittance service providers (including the Company 10 deposit service operated by Person 56 and Person 10: see paragraphs 332ff and 359ff), as well as from Crown Perth, other Australian casinos and his own bank accounts.

None of these steps were proportionate to the ML/TF risks reasonably posed by Customer 16 on and from August 2017.

Enhanced customer due diligence

1118. Having formed a suspicion for the purposes of s41 of the Act, Crown Melbourne gave the AUSTRAC CEO SMRs with respect to Customer 16 on:

a. 13 December 2017;

b. 13 February 2018;

c. 9 May 2018; and

d. 26 June 2018.

Particulars

The SMRs reported:

- suspicious losses by key players under Customer 16's junkets; and
- large transfers to and from third parties, including from other junket operators and foreign remittance service providers.

1119. On each occasion that Crown Melbourne formed a suspicion with respect to Customer 16 for the purposes of s41 of the Act, it was required to apply its ECDD program to Customer 16.

Particulars

Rule 15.9(3) of the Rules.

1120. Crown Melbourne did not carry out appropriate risk-based ECDD measures with respect to Customer 16 on each occasion that Crown Melbourne formed a suspicion with respect to Customer 16 for the purposes of s41 of the Act.

a. There are no records of ECDD being conducted following the lodgement of SMRs on 13 December 2017, 13 February 2018, 9 May 2018 and 26 June 2018: see paragraphs 664 and 685.

b. Appropriate risk-based steps were not taken to obtain or analyse information about Customer 16's source of wealth/funds: see paragraph 667.

c. Appropriate risk-based steps were not taken to analyse and monitor Customer 16's transactions – both past and future – including to understand their economic purpose: see paragraph 590 and 666.

d. On each occasion that senior management considered whether to continue the business relationship with Customer 16, senior management failed to give adequate consideration to whether the ML/TF risks posed by Customer 16 were within Crown Melbourne's risk appetite.

Particulars

Rules 15.9(3), 15.10(1)(c), (d), (2), (5) and (6) of the Rules.

See particulars to paragraph 1117.

1121. Having formed a suspicion for the purposes of s41 of the Act, Crown Perth gave the AUSTRAC CEO SMRs with respect to Customer 16 on:

a. 12 September 2017; and

b. 26 March 2019.

Particulars

The SMRs related to large transfers from third parties, including from other junket operators and foreign remittance service providers.

1122. On each occasion that Crown Perth formed a suspicion with respect to Customer 16 for the purposes of s41 of the Act, it was required to apply its ECDD program to Customer 16.

Particulars

Rule 15.9(3) of the Rules.

1123. Crown Perth did not carry out appropriate risk-based ECDD measures with respect to Customer 16 on each occasion that Crown Perth formed a suspicion with respect to Customer 16 for the purposes of s41 of the Act.

a. There are no records of ECDD being conducted following the lodgement of SMRs on 12 September 2017 and 26 March 2019: see paragraphs 664 and 685.

b. Appropriate risk-based steps were not taken to obtain or analyse information about Customer 16's source of wealth/funds: see paragraph 667.

c. Appropriate risk-based steps were not taken to analyse and monitor Customer 16's transactions – both past and future – including to understand their economic purpose: see paragraph 590 and 666.

d. On each occasion that senior management considered whether to continue the business relationship with Customer 16, senior management failed to give adequate consideration to whether the ML/TF risks posed by Customer 16 were within Crown Perth's risk appetite.

Particulars

Rules 15.9(3), 15.10(1)(c), (d), (2), (5) and (6) of the Rules.

See particulars to paragraph 1117.

1124. By reason of the matters pleaded from paragraphs 1103 to 1123, on and from August 2017, Crown Melbourne and Crown Perth:

a. did not monitor Customer 16 in relation to the provision of designated services, with a view to identifying, mitigating and managing the ML/TF risks it reasonably faced; and

b. did not do so in accordance with rr 15.5 and 15.9 of the Rules.

1125. By reason of the matters pleaded at paragraph 1124, Crown Melbourne and Crown Perth contravened s36(1) of the Act on and from August 2017 with respect to Customer 16.

Particulars

Section 36(1) of the Act is a civil penalty provision: s36(2) of the Act.

Customer 17

1126. Customer 17 has been a customer of Crown Melbourne since 26 September 1996.

1127. From at least December 2006, Crown Melbourne provided Customer 17 with designated services within the meaning of table 1 and table 3, s6 of the Act.

Particulars

On 26 September 1996, Crown Melbourne opened a credit facility (AUD/HKD) for Customer 17 which was closed on 24 November 2020. The credit facility was established with a credit limit of $3,000,000.

On 9 May 1997, Crown Melbourne opened a DAB account and safekeeping account (AUD/HKD) for Customer 17.

By 2005, Crown Melbourne recorded Customer 17's individual rated gaming activity to be a cumulative loss of $16,909,300: SMR dated 13 February 2015.

By 3 June 2018, Customer 17 had a cumulative individual turnover at Crown Melbourne of $262,000,000 with a cumulative loss of $14,000,000.

1128. Customer 17 has been a customer of Crown Perth since January 2015.

1129. From at least January 2015, Crown Perth provided Customer 17 with designated services within the meaning of table 1 and table 3, s6 of the Act.

Particulars

On 16 January 2015, Crown Perth opened an FAF account (AUD) for Customer 17 which was closed on 24 November 2020.

On 5 March 2018, Crown Perth opened a DAB account and safekeeping account (AUD) for Customer 17.

Between 14 October 2016 and 20 May 2018, Customer 17 had a cumulative individual turnover at Crown Perth of $2,000,000 with a cumulative win of $300,000.

1130. From at least 17 May 2018, Customer 17 received designated services as a junket operator, junket representative and junket player at Crown Melbourne and Crown Perth, facilitated through three different junket operators.

Particulars

On 17 May 2018, Customer 17 signed a NONEGPRA with Crown Melbourne and Crown Perth.

Customer 17 was a junket operator. At various times, Customer 17's junket program had three junket representatives.

Customer 17 was a junket representative of another junket program.

At Crown Melbourne, Customer 17 received designated services as a key player through his junket program.

By 10 October 2019, Crown Melbourne recorded Customer 17's individual gaming activity and gaming activity on junket programs run by Customer 17 as a cumulative turnover of $305,000,000 with a cumulative loss of $17,700,000

At Crown Perth, Customer 17 received designated services as a key player through his junket program, Customer 6's junkets and another junket.

By April 2019, Crown Perth recorded Customer 17's individual gaming activity and gaming activity on junket programs run by Customer 17 as a cumulative turnover of $96,000,000 with a cumulative win of $1,000,000.

The ML/TF risks posed by Customer 17

1131. By 1 March 2016, higher ML/TF risks were indicated by the nature and purpose of Customer 17's business relationship with Crown Melbourne and Crown Perth, the nature of the transactions he had been conducting, together with the suspicions Crown Melbourne itself had formed with respect to Customer 17.

Particulars

Section 36(1)(a), (b) of the Act and Chapter 15 of the Rules.

Customer 17 was a junket player. He received designated services through the channel of junket programs. This channel lacked transparency: see paragraph 477.

SMRs by 1 March 2016

By 1 March 2016, Crown Melbourne had given the AUSTRAC CEO one SMR on 13 February 2015. The SMR described Customer 17's annual losses.

By 1 March 2016, Crown Perth had not given the AUSTRAC CEO any SMRs in respect of Customer 17.

Credit applications by 1 March 2016

On 10 May 1997, Crown Melbourne approved a $4,000,000 credit limit for the purpose of an upcoming trip for Customer 17.

In advance of his first trip to Crown Perth, Customer 17 was approved for a FAF limit of $3,000,000 or HKD21,000,000. However, Customer 17 did not arrive for this trip.

Crown Melbourne approved a credit limit of $3,000,000 in respect of Customer 17 on at least two occasions. The credit profile attached copies of Customer 17's foreign passport, address, blank cheque in a foreign currency and Crown Melbourne SYCO screenshot showing credit history, and included details of Customer 17's occupation.

Due diligence by 1 March 2016

On 16 January 2015, Crown Perth conducted a risk intelligence search in respect of Customer 17, which returned that he was a foreign PEP.

On 13 February 2015, Crown Melbourne obtained a wealth report which recorded Customer 17's business interests and identified that Customer 17 had a high estimated net worth and that he was a foreign PEP.

The report also included that, in April 1995, Customer 17 was arrested in connection with perverting the course of justice. He was acquitted in May 1996. The report included that Customer 17's brother had been fined and penalised for insider trading. The report identified that Customer 17's business was involved in a joint venture which operated a casino and entertainment resort in a foreign country.

On 17 December 2015, in connection with a request to reactivate Customer 17's Crown Melbourne credit limit, a Crown Melbourne manager was described as having a strong relationship with Customer 17, having known him for 15 years.

In January 2016, Crown Melbourne and Crown Perth conducted a company search in respect of Customer 17. Crown Melbourne and Crown Perth conducted a risk intelligence search in respect of Customer 17.

1132. At all times on and from 1 March 2016, Customer 17 was a foreign PEP.

Particulars

On 16 January 2015, Crown Perth conducted a risk intelligence search in respect of Customer 17, which returned that he was a foreign PEP. Crown Perth considered Customer 17's status as a foreign PEP and approved continuing the business relationship with Customer 17.

On 13 February 2015, Crown Melbourne first determined Customer 17 to be a foreign PEP. On 31 March 2015, Crown Melbourne considered Customer 17's status as a foreign PEP and approved continuing the business relationship with Customer 17.

See paragraphs 660, 663 and 666.

1133. At all times on and from 1 March 2016, Crown Melbourne rated Customer 17's risk as high.

Particulars

Section 36(1)(a), (b) of the Act and Chapter 15 of the Rules.

On various occasions between 13 February 2015 and 22 February 2019, Crown Melbourne rated Customer 17's risk as high.

See paragraph 481.

1134. At all times on and from May 2018, Customer 17 should have been recognised by Crown Perth as a high risk customer by reason of the matters pleaded at paragraphs 1131, 1132, 1136, 1137, 1138 and 1139.

Particulars

Section 36(1)(a), (b) of the Act and Chapter 15 of the Rules.

1135. At no time was Customer 17 rated high risk by Crown Perth.

Particulars

On various occasions between 16 January 2015 and 9 May 2020, Crown Perth rated Customer 17's risk as low.

On 16 January 2015, Crown Perth identified Customer 17 to be a foreign PEP.

On 17 May 2018, Customer 17 signed a NONEGPRA with Crown Melbourne and Crown Perth.

By reason of his status as a foreign PEP and junket operator, Customer 17 should have been rated by Crown Perth as high risk.

See paragraph 481.

1136. On and from 1 March 2016 designated services provided to Customer 17 posed higher ML/TF risks including because the provision of designated services to Customer 17 involved a combination of the following factors:

a. Customer 17 was a foreign PEP: see paragraphs 118 and 663;

b. Customer 17 was a junket operator;

c. Customer 17 received high value financial and gaming services (tables 1 and 3, s6) and facilitated the provision of high value financial and gaming services (tables 1 and 3, s6) through a junket program of which he was an operator;

d. by 10 October 2019, Crown Melbourne recorded Customer 17's individual gaming activity and gaming activity on junket programs run by Customer 17 as a cumulative turnover of $305,000,000 with a cumulative loss of $17,700,000;

e. by April 2019, Crown Perth recorded Customer 17's individual gaming activity and gaming activity on junket programs run by Customer 17 as a cumulative turnover of $96,000,000 and a net win of $1,000,000;

f. designated services provided to Customer 17 lacked transparency as the services were provided through the channel of junket programs: see paragraph 477(e);

g. Customer 17 was provided with significant amounts of credit upon request, up to limits of $10,000,000 with a 'this trip only' additional limit of $15,000,000: see paragraphs 280ff and 487;

h. by 2015, Crown was aware that Customer 17 operated a foreign casino and multiple VIP gaming rooms within a foreign casino;

i. by May 2018, Crown was aware that Customer 17 was alleged to be a reputed member of an organised crime syndicate and that his brother allegedly was a senior office bearer of an organised crime syndicate; and

j. by reason of the matters set out at subparagraphs a. to i. above, there were real risks that Customer 17's source of wealth and source of funds were not legitimate.

Monitoring of Customer 17's transactions

1137. At no time did Crown Melbourne or Crown Perth appropriately monitor Customer 17's transactions on a risk-basis.

Particulars

Section 36(1)(a), (b) of the Act and rules 15.4 to 15.8 of the Rules.

Crown Melbourne and Crown Perth were unable to monitor the ML/TF risks posed by Customer 17's transactions appropriately because they did not make and keep appropriate records of designated services provided to junket players and junket operators: see paragraphs 483ff.

Crown Melbourne and Crown Perth were unable to monitor the ML/TF risks posed by transactions associated with Customer 17's junkets, including transactions by his junket representatives and key players on his junkets, because they did not make and keep appropriate records of designated services provided.

Crown Melbourne and Crown Perth did not apply appropriate risk-based transaction monitoring to designated services provided to Customer 17: see paragraphs see paragraphs 590ff, 629 to 642 and 643 to 649.

Ongoing customer due diligence

1138. On and from 1 March 2016, on multiple occasions, the provision of designated services to Customer 17 raised red flags reflective of higher ML/TF risks as a result of the provision of large amounts of credit, a table 1, s6 designated service.

Particulars

In December 2016 and October 2017, Crown Melbourne approved a $3,000,000 or HKD18,000,000 credit limit for Customer 17 in advance of a visit.

In January 2018 and March 2018, Crown Perth approved a reactivation of Customer 17's credit limit of $3,000,000 in advance of a visit.

On 23 October 2018, Crown Melbourne approved a credit limit of $10,000,000 for Customer 17's junket in advance of a visit to Crown Melbourne on 25 October 2018.

On 20 February 2019, Crown Perth approved a credit limit of $10,000,000 for Customer 17's junket.

On 9 April 2019, Crown Perth approved a credit limit of $5,000,000 for Customer 17's junket in advance of a trip commencing on 17 April 2019.

On 2 May 2019, Crown Melbourne approved a credit limit of $5,000,000 for Customer 17's junket in advance of a trip commencing on 4 May 2019.

On 9 October 2019, Crown Melbourne approved the reactivation of a credit limit of $10,000,000 with a 'this trip only' additional limit of $15,000,000 for Customer 17's junket.

1139. On and from 1 March 2016, on multiple occasions, the provision of designated services to Customer 17 raised red flags reflective of higher ML/TF risks as a result of his individual and junket gaming activity, which often involved complex, unusually large transactions and unusual patterns of transactions which had no apparent economic or visible lawful purpose.

Particulars

See paragraph 477.

Customer 17 was a junket operator and junket representative. Through Crown Perth and Crown Melbourne, he provided designated services to key players through the channel of junket programs: see paragraph 483ff.

Individual gaming activity

Between 14 October 2016 and 20 May 2018, Customer 17 had an individual turnover at Crown Perth of $2,000,000 with a win of $300,000.

By 3 June 2018, Customer 17 had a cumulative individual turnover at Crown Melbourne of $262,000,000 with a cumulative loss of $14,000,000.

Junket activity

On 17 May 2018, Customer 17 signed a NONEGPRA with Crown Melbourne and Crown Perth. However, his junket was not approved until 4 June 2018.

On 21 May 2018, Customer 17's junket application was provided to Crown Melbourne together with several attachments, including proof of address, identification and passport details. The application was rejected because Crown considered that Customer 17 would not bring new customers to Crown Melbourne. There is no indication that Crown Melbourne considered the high ML/TF risk posed by Customer 17 when assessing the application.

On 28 May 2018, the Credit control team was advised of Customer 17's new junket operator application and requested that the due diligence process be started.

On 4 June 2018, Crown Melbourne approved Customer 17 to commence junket operations despite the high ML/TF risk posed by Customer 17.

Between 27 October 2018 and 1 November 2018, Customer 17 operated and was a key player in a junket program at Crown Melbourne with a turnover of $11,614,800 and win of $1,033,975. Customer 17's turnover as a key player in his junket was $3,583,600 with a win of $213,500.

Between 22 February 2019 and 7 March 2019, Customer 17 operated a junket at Crown Perth with a turnover of $65,159,300 with a loss of $284,275.

By 26 April 2019, Customer 17 had a cumulative turnover at Crown Melbourne of $273,000,000 with a loss of $13,100,000. Customer 17 had a cumulative turnover at Crown Perth of $96,000,000 and a net win of $1,000,000.

Between 4 May 2019 and 13 May 2019, Customer 17 operated a junket at Crown Melbourne with a turnover of $31,941,600 and win of $4,844,050.

By 10 October 2019, Customer 17 had a cumulative turnover at Crown Melbourne of $305,000,000 with a loss of $17,700,000. Customer 17 had not increased his turnover at Crown Perth.

Between 10 October 2019 and 13 October 2019, Customer 17 operated a junket program at Crown Melbourne with an estimated turnover of $9,234,600 and estimated loss $849,685.

On 14 May 2020, Crown Melbourne sent a $3,493,810 telegraphic transfer to Crown Perth for the credit of Customer 17's Crown Perth DAB account.

1140. At no time did Crown Melbourne or Crown Perth undertake appropriate risk-based customer due diligence with respect to Customer 17 with a view to identifying, mitigating and managing the ML/TF risks posed by the provision of designated services on and from 1 March 2016.

a. At no time did Crown Melbourne or Crown Perth take appropriate steps to understand whether Customer 17's source of wealth/funds was legitimate.

b. At no time did Crown Melbourne or Crown Perth take appropriate steps to identify or analyse the ML/TF risks of Customer 17's transactions or to consider whether they had a lawful purpose.

c. At no time did Crown Melbourne or Crown Perth give appropriate consideration to whether large and high risk transactions should be processed.

d. On each occasion that senior management considered whether to continue the business relationship with Customer 17, senior management failed to give adequate consideration to whether the ML/TF risks posed by Customer 17 were within Crown Melbourne or Crown Perth's risk appetite.

Particulars

Section 36(1)(a) of the Act.

The due diligence steps taken with respect to Customer 17 included:

Wealth and risk intelligence reports

In May 2016, June 2016, September 2016, October 2017, May 2018, May 2019, Crown Melbourne and Crown Perth obtained wealth reports in respect of Customer 17. The wealth reports included Customer 17's net worth, business interests and the foreign public positions he formerly held.

In May 2018 and April 2019, Crown Aspinalls obtained a risk intelligence report in respect of Customer 17 which was provided to Crown Melbourne and Crown Perth. The reports included Customer 17's net worth and business interests, that Customer 17 was a foreign PEP by association and in his own capacity, that a May 2009 report published by a foreign gaming commission alleged that Customer 17 was a reputed member of an organised crime syndicate and that his brother allegedly was a senior office bearer of an organised crime syndicate, that Customer 17 was a director of an offshore company, that Customer 17 oversaw the strategic development of a casino joint venture and that jurisdictional risk factors were associated with Customer 17 due to the lack of transparency, high money-laundering risk and high corruption perception in country of origin and residence.

Senior management did not appropriately consider this report when determining whether a continuing business relationship was within Crown's ML/TF risk appetite.

Database searches

In December 2016, August 2017, February 2018, February 2018, May 2018, October 2018, May 2019 and March 2020, Crown Perth conducted risk intelligence searches which identified Customer 17 to be an inactive foreign PEP.

On numerous occasions between March 2016 and March 2020, Crown conducted various searches in respect of companies that Customer 17 was associated with.

At no point, as a result of these searches, did Crown Melbourne or Crown Perth appropriately consider the ML/TF risks of the source of Customer 17's wealth/funds or whether an ongoing business relationship with Customer 17 was within their ML/TF risk appetite.

Customer 17's application to become a junket operator

In May 2018, Customer 17's application to become a junket operator at Crown Melbourne was rejected because Customer 17 was considered not to be likely to bring new customers to Crown. There is no indication that Crown Melbourne considered the high ML/TF risk posed by Customer 17 when assessing the application.

In May 2018 and June 2018, Customer 17 applied to be a junket operator at Crown Melbourne. In assessing Customer 17's applications, Crown Melbourne senior management considered Customer 17's historic turnover at Crown Perth and Crown Melbourne, Customer 17's lines of credit at other casinos in Australia and internationally and Customer 17's business interests including that he was involved in a joint venture that operated a casino and entertainment complex.

On 4 June 2018, Crown Melbourne senior management approved Customer 17's application to be a junket operator.

2019 junket profiles

In April 2019, October 2019 and December 2019, Crown prepared a profile in respect of Customer 17's junket. The profiles included Customer 17's turnover at Crown Melbourne and Crown Perth, searches conducted in 2018 and 2019 in respect of Customer 17 and that Customer 17 had a police check issued in February 2019. The ultimate recommendation was that Crown Melbourne continue to conduct business with him. However, the junket profiles did not engage with the ML/TF risk posed by Customer 17 and the recommendation did not appropriately consider the ML/TF risks posed by Customer 17.

None of these steps were proportionate to the ML/TF risks reasonably posed by Customer 17 on and from 1 March 2016.

1141. Between at least April 1993 and January 2007, a number of widely accessible media reports were published in respect of Customer 17. These articles do not appear to have come to Crown Melbourne or Crown Perth's attention as part of its due diligence process.

Particulars

The media reports concerned Customer 17's business interests, allegations of market manipulation by minority shareholders in Customer 17's company, allegations that Customer 17's company had lost a significant amount of money on their behalf,

Customer 17's brother's arrest and charge in connection with an assault and Customer 17's arrest in connection with perverting the course of justice.

The media reports also related to VIP gaming halls operated within a casino by Customer 17, which reportedly had a very high average turnover in 2005, and the joint venture in which Customer 17 was involved to develop and operate another casino and entertainment complex.

Enhanced customer due diligence

1142. Despite the high ML/TF risks posed by the provision of designated services to Customer 17 pleaded at paragraph 1136, at no point on and from 1 March 2016 did Crown Melbourne or Crown Perth give the AUSTRAC CEO an SMR in respect of Customer 17.

1143. At all times from 1 March 2016, Customer 17 was a foreign PEP.

Particulars

Section 36(1)(a) of the Act

See particulars to paragraph 1132.

1144. At all times from 1 March 2016, Crown Melbourne and Crown Perth were required to apply its ECDD program to Customer 17.

Particulars

Rules 15.9(2) and 15.11 of the Rules

1145. Crown Melbourne and Crown Perth did not carry out appropriate risk-based ECDD measures with respect to Customer 17 on and from 1 March 2016 given his status as a foreign PEP. In particular:

a. Crown Melbourne and Crown Perth did not undertake a detailed analysis of Customer 17's KYC information or analyse the legitimacy of Customer 17's source of wealth/funds;

b. senior management approval for Crown Melbourne and Crown Perth to continue a business relationship with Customer 17 did not give adequate consideration to the ML/TF risks posed by the customer; and

c. senior management approval for Crown Melbourne and Crown Perth to continue to provide designated services to Customer 17 did not give adequate consideration to the ML/TF risks posed by the customer.

Particulars

Rules 15.10(2), 15.10(6), 15.11 of the Rules.

Crown conducted a number of searches in advance of activating or reactivating Customer 17's credit facility at Crown Melbourne and Crown Perth, approving Customer 17's junket at Crown Melbourne and Crown Perth and preparing a junket profile in respect of Customer 17. However, none of these searches were conducted with a view to determining ML/TF risk and the decisions to activate or

reactivate the credit facility, as well as to approve his junket, were not considered in the context of that risk.

The junket profiles prepared in 2019 related only to Customer 17's operation of a junket program, and not to his overall business relationship with Crown Melbourne or Crown Perth.

See particulars to paragraph 1140.

See paragraph 660, 663, 666, 667 and 668.

1146. On and from 1 March 2016, Crown Melbourne rated Customer 17 high risk.

Particulars

On five occasions between 13 February 2015 and 22 February 2019, Crown Melbourne rated Customer 17's risk as high: see paragraph 1133.

1147. On each occasion that Crown Melbourne rated Customer 17 high risk, Crown Melbourne was required to apply its ECDD program to Customer 17.

Particulars

Rule 15.9(1) of the Rules.

See paragraph 661.

1148. Crown Melbourne did not carry out appropriate risk-based ECDD measures with respect to Customer 17 on each occasion that Crown Melbourne rated Customer 17 high risk.

Particulars

At no time did Crown Melbourne conduct ECDD following each occasion that it rated Customer 15 high risk: see paragraph 1145.

See paragraphs 661, 666, 667 and 668.

1149. By reason of the matters pleaded from paragraphs 1126 to 1148, on and from 1 March 2016, Crown Melbourne and Crown Perth:

a. did not monitor Customer 17 in relation to the provision of designated services, with a view to identifying, mitigating and managing the ML/TF risks it reasonably faced; and

b. did not do so in accordance with rr 15.5 and 15.9 of the Rules.

1150. By reason of the matters pleaded at paragraph 1149, Crown Melbourne and Crown Perth contravened s36(1) of the Act on and from 1 March 2016 with respect to Customer 17.

Particulars

Section 36(1) of the Act is a civil penalty provision: s36(2) of the Act.

Customer 18

1151. Customer 18 has been a customer of Crown Melbourne since 10 September 2015.

1152. From at least 27 October 2015, Crown Melbourne provided Customer 18 with designated services within the meaning of table 1 and table 3, s6 of the Act.

1153. From at least 26 July 2017, Customer 18 received designated services as a junket player, facilitated through two different junket operators, and as a junket operator at Crown Melbourne.

Particulars to paragraphs 1152 and 1153

On 8 September 2015, Crown Melbourne entered into a NONEGPRA with Customer 18 to operate junkets at Crown Melbourne.

Customer 18 received designated services as a junket player under his own junket program and two other junket programs.

On 27 October 2015, Crown Melbourne approved a credit facility (AUD/HKD) for Customer 18. On 24 November 2020, Crown Melbourne closed the credit facility.

On 12 February 2017, Crown Melbourne opened a DAB account and safekeeping account for Customer 18.

1154. Customer 18 has been a customer of Crown Perth since 5 August 2006.

1155. From at least 5 August 2006, Crown Perth provided Customer 18 with designated services within the meaning of table 1 and table 3, s6 of the Act.

1156. From at least 31 July 2016, Customer 18 received designated services as a junket player, facilitated through two different junket operators, and as a junket operator at Crown Perth.

Particulars to paragraphs 1155 and 1156

On 5 August 2006, Crown Perth opened a DAB account and safekeeping account for Customer 18.

On 3 August 2015, Crown Perth opened a second DAB account and safekeeping account for Customer 18 under a second PID. On 30 October 2015, Crown Perth opened a third DAB account and safekeeping account for Customer 18 under a third PID.

On 18 November 2015, Crown Perth approved a credit facility (AUD/HKD) for Customer 18 under each of Customer 18's three PIDs. On 28 June 2021, Crown Perth closed the credit facility.

On 24 March 2016, Crown Melbourne entered into a NONEGPRA with Customer 18 to operate junkets at Crown Perth.

The ML/TF risks posed by Customer 18

1157. On and from mid to late 2017, designated services provided to Customer 18 posed higher ML/TF risks including because the provision of designated services to Customer 18 involved a combination of the following factors:

a. Customer 18 was a junket operator;

b. Customer 18 was a junket player;

c. Customer 18 received high value financial (table 1, s6) and gaming services (table 3, s6) provided through multiple junket programs: see paragraph 473ff;

d. Customer 18 was a junket operator who facilitated the provision of high value financial and gaming services (tables 1 and 3, s6) to key players on his junket programs: see paragraph 473ff;

e. by no later than April 2019, Crown Melbourne recorded that turnover on junket programs operated by Customer 18 at Crown Melbourne had exceeded $584,000,000;

f. by no later than April 2019, Crown Perth recorded that turnover on junket programs operated by Customer 18 at Crown Perth had exceeded $60,000,000;

g. designated services provided to Customer 18 lacked transparency as the services were provided through the channel of junket programs: see paragraph 477(e);

h. the table 3, s6, designated services provided to Customer 18 involved escalating rates of high turnover;

i. designated services provided to Customer 18 involved large transfers to and from third parties, including from foreign remittance service providers: see paragraph 456ff. Between August and September 2018, Crown Melbourne received approximately $16,000,000 across 32 separate transfers from a foreign remittance service provider for the benefit of Customer 18;

j. designated services provided to Customer 18 involved large cross-border movements of funds, including through a Southbank account: see paragraph 239;

k. large amounts of funds were transferred to and from Customer 18's bank accounts and his DAB account, and to and from other customers' DAB accounts, involving the provision by Crown Melbourne of designated services within the meaning of items 31 and 32, table 1, s6 of the Act;

l. from 7 June 2019, Customer 18 had significant parked or dormant funds of $4,940,671 in his DAB accounts: see paragraph 252;

m. in 2018, Customer 18 was the subject of law enforcement inquiries; and

n. by reason of the matters set out at subparagraphs a. to m. above, there were real risks that Customer 18's source of wealth/funds were not legitimate.

1158. At all times on and from mid to late 2017, Customer 18 should have been recognised by Crown Melbourne as a high risk customer by reason of the matters pleaded at paragraphs 1157, 1162, 1163, 1164, 1167 and 1170.

Particulars

Section 36(1)(a), (b) of the Act and Chapter 15 of the Rules.

On 24 July 2017, Crown Melbourne assessed and rated Customer 18 moderate risk.

On various occasions between 30 May 2018 and 29 November 2018, Crown Melbourne assessed and rated Customer 18 significant risk.

This was despite Customer 18's high turnover under junket programs that he operated, several large transactions from foreign remittance services and transactions with references which indicated that the funds were not for gaming activity.

See paragraph 481.

1159. At no time was Customer 18 rated high risk by Crown Melbourne.

1160. At all times on and from mid to late 2017, Customer 18 should have been recognised by Crown Perth as a high risk customer by reason of the matters pleaded at paragraphs 1157, 1162, 1163, 1164, 1165 and 1171.

Particulars

Section 36(1)(a), (b) of the Act and Chapter 15 of the Rules.

On 15 November 2017, Crown Perth assessed and rated Customer 18 moderate risk.

This was despite Customer 18's high turnover under junket programs that he operated, several large transactions from foreign remittance services and transactions with references which indicated that the funds were not for gaming activity.

See paragraph 481.

1161. At no time was Customer 18 rated high risk by Crown Perth.

Monitoring of Customer 18's transactions

1162. At no time did Crown Melbourne or Crown Perth appropriately monitor Customer 18's transactions on a risk-basis.

Particulars

Section 36(1)(a), (b) of the Act and rules 15.4 to 15.8 of the Rules.

Crown Melbourne and Crown Perth were unable to monitor the ML/TF risks posed by Customer 18's transactions appropriately because they did not make and keep appropriate records of designated services provided to junket players or operators: see paragraphs 483ff.

Crown Melbourne and Crown Perth did not apply appropriate risk-based transaction monitoring to designated services provided to Customer 18: see paragraphs 590ff, 629 to 642 and 643 to 649.

Customer 18's transactions involved repeated transactions indicative of ML/TF typologies and vulnerabilities that were not detected prior to a 2021 lookback. Had appropriate risk-based transaction monitoring been applied, these transactions could have been identified earlier: see paragraphs 686 and 687.

Transactions involving Customer 18 were identified as indicative of the ML/TF typology of parked funds by an independent auditor in 2021. As at 30 April 2021, Customer 18 had parked $4,940,671 in his safekeeping account for 693 days with the last transaction on the account occurring on 7 June 2019.

In 2020, an independent expert identified six deposits into a Southbank account from foreign remittance service providers for the credit of Customer 18 between 4 August 2017 and 26 July 2018,

totalling $1,575,088. These transactions were indicative of the ML/TF typology of the use of third party remitters:

- From 3 August 2017 to 4 August 2017, Crown Melbourne received two telegraphic transfers for the credit of Customer 18 totalling $152,251; and
- Between 10 July 2018 and 26 July 2018, Crown Melbourne received five telegraphic transfers totalling $1,499,815 for the credit of Customer 18.

The independent expert also identified an additional deposit of $76,978 from a third party for the credit of Customer 18 with a payment reference 'payment of business' on 3 August 2017.

Ongoing customer due diligence

1163. On and from mid-2017, on multiple occasions, the provision of designated services to Customer 18 by Crown Melbourne and Crown Perth raised red flags reflective of higher ML/TF risks as a result of Customer 18's junket activity.

Particulars

See paragraph 477.

Total gaming activity on junket programs

By April 2019, Crown Melbourne recorded that gaming activity on junket programs operated by Customer 18 at Crown Melbourne involved a total turnover of approximately $584,000,000 with losses of $10,200,000.

By April 2019, Crown Perth recorded that gaming activity on junket programs operated by Customer 18 at Crown Perth involved a total turnover of approximately $60,000,000 with losses of $400,000.

Junket activity in 2016

Customer 18 operated junket programs at Crown Perth between 31 July 2016 and 12 April 2017, which involved a turnover of at least $14,000,000.

Junket activity in 2017

Customer 18 operated junket programs at Crown Perth in April 2017 and August 2017.

Customer 18 operated a junket program at Crown Melbourne in July 2017. Crown Melbourne noted high losses noted for two key players on Customer 18's junket program, totalling $210,950: SMR dated 24 July 2017.

Junket activity in 2018.

On 7 July 2018, Customer 18 ran a junket program at Crown Melbourne. The buy-in was $3,500,000 with a turnover of $98,512,200 and losses of $759,885. Commissions of $788,098 were payable by Crown Melbourne to Customer 18, along with use of the

Crown private jet to fly the junket's key players to and from Crown Melbourne: see paragraphs 454 and 491(c). Crown Melbourne noted high losses noted for three key players on Customer 18's junket program, totalling $1,525,650: SMR dated 18 July 2018.

On 26 July 2018, Customer 18 ran a junket program at Crown Melbourne. The buy-in was $15,000,000 with a turnover of $144,474,000 and losses of $5,351,750. Commissions of $3,211,050 were payable by Crown Melbourne to Customer 18. Crown Melbourne noted high losses for two key players on Customer 18's junket program, totalling HKD5,020,150: SMR dated 8 August 2018.

On 13 August 2018, Customer 18 ran a junket program at Crown Melbourne. The buy-in was $13,000,000 with a turnover of $450,055,000 and losses of $14,779,065. Commissions of $3,600,440 were payable by Crown Melbourne to Customer 18. Crown Melbourne noted high losses for six key players on Customer 18's junket program, totalling $13,770,130, including losses of $10,743,000 noted for a single key player: SMR dated 24 August 2018.

In 2018, gaming activity on junket programs operated by Customer 18 at Crown Melbourne involved a cumulative turnover of $575,032,046 with a cumulative loss of $15,048,486.

1164. On and from mid to late 2017, on multiple occasions, the provision of designated services to Customer 18 by Crown Melbourne and Crown Perth raised red flags reflective of higher ML/TF risks as a result of unusual transactions and patterns of transactions involving Customer 18 and foreign remittance service providers.

Particulars

See paragraphs 420ff and 456ff.

On the following dates, designated services provided to Customer 18 involved complex, unusually large transactions and unusual patterns of transactions which had no apparent economic or visible lawful purpose:

Unusual transactions and patterns of transactions in 2016

On 4 June 2016, a third party deposited $43,928 into her Crown Melbourne DAB account, then transferred the funds to Customer 18's DAB account: SMR dated 5 June 2018.

On 28 July 2016, a key player on Customer 18's junket cashed out AU$20,070 in cash chips in circumstances where the junket program was only using program chips and Crown Melbourne was unable to confirm any play: SMR dated 29 July 2016.

Unusual transactions and patterns of transactions in 2018

Between 9 August 2018 and 18 September 2018, 32 telegraphic transfers in amounts between $200,000 and $320,000 were received by Crown Melbourne for the benefit of Customer 18, from a third party foreign remittance service provider, totalling approximately

$16,000,000. Of this, $13,000,000 was used as front money for a junket program between 13 August and 23 August 2018: SMR dated 28 November 2018.

On 23 October 2018, Customer 18 arranged for a telegraphic transfer of $788,098 from his Crown Melbourne DAB account to his Australian bank account.

On 27 November 2018, Customer 18 arranged for a telegraphic transfer of $577,672 from his Crown Melbourne DAB account to his Australian bank account.

1165. From 30 May 2018, inquiries by law enforcement agencies relating to Customer 18 raised red flags reflective of higher ML/TF risks for the provision of designated services to Customer 18.

Particulars

On 30 May 2018, Crown Melbourne received a law enforcement inquiry in relation to Customer 18. Following receipt of the inquiry, Crown Melbourne increased Customer 18's risk rating to significant.

1166. At no time did Crown Melbourne or Crown Perth undertake appropriate risk-based customer due diligence with respect to Customer 18 with a view to identifying, mitigating and managing the ML/TF risks posed by the provision of designated services on and from mid to late 2017.

a. At no time did Crown Melbourne or Crown Perth take appropriate steps to understand whether Customer 18's source of wealth/funds was legitimate.

b. At no time did Crown Melbourne or Crown Perth take appropriate steps to identify or analyse the ML/TF risks of Customer 18's transactions or to consider whether they had a lawful purpose.

c. On each occasion that senior management considered whether to continue the business relationship with Customer 18, senior management failed to give adequate consideration to whether the ML/TF risks posed by Customer 18 were within Crown Melbourne or Crown Perth's risk appetite.

Particulars

Section 36(1)(a) of the Act.

The due diligence steps taken with respect to Customer 18 included:

Database searches

On 21 March 2016, 22 December 2016, 30 March 2017, 20 October 2017, 23 April 2018, 5 April 2019 and 21 October 2019, the Credit control team performed risk intelligence searches on Customer 18.

On 22 December 2016, 29 March 2017, 24 April 2018, 3 September 2018, 8 May 2019 and 26 July 2019, the Credit control team conducted company and property searches on companies linked to Customer 18.

At no point, as a result of these searches, did Crown Melbourne or Crown Perth appropriately consider the ML/TF risks of the source of

Customer 18's wealth/funds or whether an ongoing business relationship with Customer 18 was within their ML/TF risk appetite.

Wealth reports

On 16 May 2016, 22 December 2016, 3 January 2017 and 12 September 2019, the Credit control team obtained wealth reports on Customer 18 which reported on his business interests and involvement in gaming tournaments.

Junket profile

By 13 April 2017, the Credit control team drafted a junket profile for the purpose of assessing Customer 18's creditworthiness. The profile recommended that Crown continue to conduct business subject to a police clearance.

The profile was updated on 12 May 2017 with Customer 18's police clearance and updated again on 10 April 2019. Each update recommended that Crown continue to conduct business with Customer 18.

The profiles did not appropriately considered the high ML/TF risk posed by Customer 18.

Senior management engagement

In early 2017, the VIP Operations Committee meeting attended by a Crown Resorts director, the Chief Executive Officer (Australian Resorts), the Senior Vice President (International Business), the Group General Manager (International Business Operations) and the Chief Legal Officer (Australian Resorts) considered Customer 18's junket profile. The minutes of the meeting recorded a decision to continue to conduct business subject to receipt of a police clearance.

There was no subsequent senior management consideration of Crown's business relationship with Customer 18 on and from mid to late 2017.

None of these steps were proportionate to the ML/TF risks reasonably posed by Customer 18 on and from mid to late 2017.

Enhanced customer due diligence

1167. Having formed a suspicion for the purposes of s41 of the Act, Crown Melbourne gave the AUSTRAC CEO SMRs with respect to Customer 18 on:

a. 24 July 2017;

b. 5 June 2018;

c. 18 July 2018;

d. 2 August 2018;

e. 24 August 2018; and

f. 28 November 2018.

Particulars

The SMRs reported:

- high losses for key players on Customer 18's junkets;
- transfers from third parties to Customer 18's DAB account; and
- large telegraphic transfers from Customer 18's DAB account to third parties.

1168. On each occasion that Crown Melbourne formed a suspicion with respect to Customer 18 for the purposes of s41 of the Act, it was required to apply its ECDD program to Customer 18.

Particulars

Rule 15.9(3) of the Rules.

1169. Crown Melbourne did not carry out appropriate risk-based ECDD measures with respect to Customer 18 on each occasion that Crown Melbourne formed a suspicion with respect to Customer 18 for the purposes of s41 of the Act.

a. There are no records of ECDD being conducted following the lodgement of SMRs on 24 July 2017, 5 June 2018, 18 July 2018, 2 August 2018, 24 August 2018 and 28 November 2018: see paragraphs 664 and 685.

b. Appropriate risk-based steps were not taken to obtain or analyse information about Customer 18's source of wealth/funds: see paragraph 667.

c. Appropriate risk-based steps were not taken to analyse and monitor Customer 18's transactions – both past and future – including to understand their economic purpose: see paragraph 590 and 666.

d. On each occasion that senior management considered whether to continue the business relationship with Customer 18, senior management failed to give adequate consideration to whether the ML/TF risks posed by Customer 18 were within Crown Melbourne's risk appetite.

Particulars

Rules 15.9(3), 15.10(1)(c), (d), (2), (5) and (6) of the Rules.

After lodging the SMR on 24 August 2018, the CTRM reviewed the SYCO records of key players in Customer 18's junket. The CTRM requested further information be obtained on the key players however he was not provided with any further information. These steps were not adequate ECDD following the lodgement of the 24 August 2018 SMR.

See particulars to paragraph 1166.

1170. Having formed a suspicion for the purposes of s41 of the Act, Crown Perth gave the AUSTRAC CEO an SMR with respect to Customer 18 on 29 July 2016.

Particulars

The SMR related to a cash out of AU$20,070 in cash chips by a key player on Customer 18's junket, when the junket program was using HKD program chips.

1171. On each occasion that Crown Perth formed a suspicion with respect to Customer 18 for the purposes of s41 of the Act, it was required to apply its ECDD program to Customer 18.

Particulars

Rule 15.9(3) of the Rules.

1172. Crown Perth did not carry out appropriate risk-based ECDD measures with respect to Customer 18 on each occasion that Crown Perth formed a suspicion with respect to Customer 18 for the purposes of s41 of the Act.

a. There are no records of ECDD being conducted following the lodgement of SMRs on 29 July 2016: see paragraphs 664 and 685.

b. Appropriate risk-based steps were not taken to obtain or analyse information about Customer 18's source of wealth/funds: see paragraph 667.

c. Appropriate risk-based steps were not taken to analyse and monitor Customer 18's transactions – both past and future – including to understand their economic purpose: see paragraph 590 and 666.

d. On each occasion that senior management considered whether to continue the business relationship with Customer 18, senior management failed to give adequate consideration to whether the ML/TF risks posed by Customer 18 were within Crown Perth's risk appetite.

Particulars

Rules 15.9(3), 15.10(1)(c), (d), (2), (5) and (6) of the Rules.

See particulars to paragraph 1166.

1173. By reason of the matters pleaded from paragraphs 1151 to 1172, on and from mid to late 2017, Crown Melbourne and Crown Perth:

a. did not monitor Customer 18 in relation to the provision of designated services, with a view to identifying, mitigating and managing the ML/TF risks it reasonably faced; and

b. did not do so in accordance with rr 15.5 and 15.9 of the Rules.

1174. By reason of the matters pleaded at paragraph 1173, Crown Melbourne and Crown Perth contravened s36(1) of the Act on and from mid to late 2017 with respect to Customer 18.

Particulars

Section 36(1) of the Act is a civil penalty provision: s36(2) of the Act.

Customer 19

1175. Customer 19 has been a customer of Crown Melbourne since 3 February 2009.

1176. From at least 3 February 2009, Crown Melbourne provided Customer 19 with designated services within the meaning of table 1 and table 3, s6 of the Act.

Particulars

On 3 February 2009, Crown Melbourne opened a DAB account and safekeeping account (AUD/HKD) for Customer 19, which remain open.

On 5 November 2014, Crown Melbourne opened a credit facility (AUD/HKD) for Customer 19, which was closed on 23 November 2020.

On 26 February 2015, Crown Melbourne opened a DAB account and safekeeping account (AUD) for Customer 19, which were closed on 23 November 2020.

1177. From at least 2014, Customer 19 received designated services as a junket operator and junket player facilitated through one junket program at Crown Melbourne.

Particulars

Customer 19 was a junket operator and a key player in his junket.

On various occasions, there were seven junket representatives of Customer 19's junket program .

By 17 March 2020, Customer 19's junket program had a turnover at Crown Melbourne of $1,500,000,000 and net Crown win of $5,500,000.

By December 2019, as a key player in his junket program at Crown Melbourne and Crown Perth, Customer 19 personally had a cumulative recorded turnover of $44,800,000 with a cumulative loss of $6,500,000.

1178. Customer 19 has been a customer of Crown Perth since 2 October 2015.

1179. From 2 October 2015, Crown Perth provided Customer 19 with designated services within the meaning of table 1 and table 3, s6 of the Act.

Particulars

On 2 October 2015, Crown Perth opened a DAB account and safekeeping account (AUD) for Customer 19, which remains open.

On 30 October 2015, Crown Perth opened an FAF account (AUD) for Customer 19, which was closed on 23 November 2020.

1180. From at least 2014, Customer 19 received designated services as a junket operator and junket player facilitated through one junket program at Crown Perth.

Particulars

Customer 19 was a junket operator and a key player in his junket.

On various occasions, there were seven junket representatives of Customer 19's junket program.

By 17 March 2020, Customer 19's junket program had a turnover at Crown Perth of $200,000,000 and net Crown win of $7,700,000.

By December 2019, as a key player in his junket program at Crown Melbourne and Crown Perth, Customer 19 personally had a recorded cumulative turnover of $44,800,000 with a cumulative loss of $6,500,000.

The ML/TF risks posed by Customer 19

1181. By 1 March 2016, higher ML/TF risks were indicated by the nature and purpose of Customer 19's business relationship with Crown Melbourne and Crown Perth, the nature of the transactions he had been conducting, together with the suspicions Crown Melbourne itself had formed with respect to Customer 19.

Particulars

Section 36(1)(a), (b) of the Act and Chapter 15 of the Rules.

Customer 19 was a junket operator and a junket player. He received designated services through the channel of junket programs. This channel lacked transparency: see paragraph 477.

SMRs by 1 March 2016

By 1 March 2016, Crown Melbourne had given the AUSTRAC CEO six SMRs in relation to Customer 19 – on 11 December 2014, two SMRs on 10 March 2015, 14 July 2015, 1 October 2015 and 6 January 2016. The SMRs described significant losses of key players in Customer 19's junket program, annual losses of key players in Customer 19's junket, telegraphic transfers from third parties not listed as key players in Customer 19's junket program and the amount of cash key players in Customer 19's junket were prepared to carry.

Junket activity by 1 March 2016

On 19 February 2015, Customer 19 was approved for a credit facility of $15,000,000 for the purpose of junket programs that he operated in February 2015, being the largest credit limit approved in respect of Customer 19.

In 2015, Customer 19 operated at least four junket programs at Crown Melbourne. SMRs given to the AUSTRAC CEO in 2015 identified losses totalling $4,478,780 and HKD33,499,550. Customer 19 was a key player in one of the junket programs and had a personal loss of HKD5,325,500.

Large and suspicious transactions by 1 March 2016

By 1 March 2016, Customer 19 had engaged in a number of large transactions at Crown Melbourne:

- on 8 March 2015, Customer 19 made a chip cash in of $400,000;
- on 22 May 2015, Customer 19 transferred $1,237,040 from his personal bank account to a Southbank account;
- on 25 August 2015, Customer 19 transferred $2,051,585 from his personal bank account to a Southbank account;

- on 29 September 2015, Customer 19's junket received a telegraphic transfer of a large sum in a foreign currency from a third party not listed as a key player under any recent junket program: SMR dated 1 October 2015;
- on 5 January 2016, Customer 19's junket received a telegraphic transfer of a large sum in a foreign currency from a third party not listed as a key player under any recent junket program: SMR dated 6 January 2016; and
- on 19 January 2016, Customer 19 transferred $2,400,000 from his personal account to a Southbank account.

By 1 March 2016, Customer 19 had engaged in at least one large transaction at Crown Perth:

- on 19 January 2016, Customer 19 transferred $3,702,256 from his personal account to a Riverbank account.

Due diligence conducted by 1 March 2016

In March 2015, Crown Melbourne obtained a number of reports in respect of Customer 19 which identified his business interests in a foreign country. The reports estimated Customer 19's high net worth.

1182. As at 1 March 2016, Customer 19 should have been recognised by Crown Melbourne as a high risk customer for the reasons pleaded at paragraph 1181 and as a result of his PEP status pleaded in paragraph 1195.

1183. At all times on and from 1 March 2016, Customer 19 should have been recognised by Crown Melbourne as a high risk customer by reason of the matters pleaded at paragraphs 1181, 1188, 1189, 1190, 1192 and 1195.

Particulars

Section 36(1)(a), (b) of the Act and Chapter 15 of the Rules.

1184. At no time was Customer 19 rated high risk by Crown Melbourne.

Particulars

On various occasions between 11 December 2014 and 22 July 2016, Customer 19 was rated moderate risk by Crown Melbourne.

Customer 19's risk was not assessed by Crown Melbourne after 22 July 2016, despite being a junket operator who received designated services at Crown Melbourne with a turnover of $1,500,000,000 by March 2020.

See paragraph 481.

1185. As at 1 March 2016, Customer 19 should have been recognised by Crown Perth as a high risk customer for the reasons pleaded at paragraph 1181 and as a result of his PEP status pleaded in paragraph 1195.

1186. At all times on and from 1 March 2016, Customer 19 should have been recognised by Crown Perth as a high risk customer by reason of the matters pleaded at paragraphs 1181, 1188, 1189, 1190 and 1195.

Particulars

Section 36(1)(a), (b) of the Act and Chapter 15 of the Rules.

1187. At no time was Customer 19 rated high risk by Crown Perth.

Particulars

On 15 November 2021, Customer 19 was rated moderate risk by Crown Perth for the first time. Customer 19's risk was not assessed by Crown Perth between 2 October 2015 and 20 September 2016, despite being a junket operator who received designated services at Crown Perth with a turnover of $200,000,000 by October 2016.

See paragraph 481.

1188. On and from 1 March 2016 designated services provided to Customer 19 posed higher ML/TF risks including because the provision of designated services to Customer 19 involved a combination of the following factors:

a. Customer 19 was a foreign PEP: see paragraphs 118 and 663;

b. Customer 19 was a junket operator and a junket player;

c. Customer 19 was a junket operator who facilitated the provision of high value financial and gaming services (tables 1 and 3, s6) to several players (including foreign PEPs) on his junket programs: see paragraph 473ff;

d. by March 2020, Customer 19's junket program had a turnover at Crown Melbourne of $1,500,000,000 with a loss of $5,500,000;

e. by March 2020, Customer 19's junket program had a turnover at Crown Perth of $200,000,000 with a loss of $7,700,000;

f. by December 2019, as a key player on his own junket programs at Crown Melbourne and Crown Perth, Customer 19 personally had a cumulative turnover of $44,800,000 with a loss of $6,500,000;

g. designated services provided to Customer 19 lacked transparency as the services were provided through the channel of junket programs: see paragraph 477(e);

h. Customer 19 was provided with significant amounts of credit with respect to junket programs that he facilitated: see paragraphs 280ff and 487;

i. designated services provided to Customer 19 involved large transfers to and from third parties: see paragraph 456ff;

j. designated services provided to Customer 19 involved large cross-border movements of funds: see paragraph 238(d);

k. in 2019, Crown approved a credit facility for Customer 19 on the condition that any net winnings of the junket program be paid to Crown Aspinalls towards a debt incurred by a key player in Customer 19's junket who was a foreign PEP;

l. at various times, Customer 19 had significant parked or dormant funds in his DAB accounts: see paragraph 252;

m. Crown Melbourne made available the Crown private jet for Customer 19. There were inadequate controls on the carrying of large amounts of cash on Crown's private jets: see paragraphs 454 and 491(c);

n. from at least 28 June 2010, media reports identified Customer 19 as a person connected to organised crime; and

o. by reason of the matters set out at subparagraphs a. to n. above, there were real risks that Customer 19's source of wealth and source of funds were not legitimate.

Monitoring of Customer 19's transactions

1189. At no time did Crown Melbourne and Crown Perth appropriately monitor Customer 19's transactions on a risk-basis.

Particulars

Section 36(1)(a), (b) of the Act and rules 15.4 to 15.8 of the Rules.

Crown Melbourne and Crown Perth were unable to monitor the ML/TF risks posed by Customer 19's transactions appropriately because they did not make and keep appropriate records of designated services provided to junket players in Customer 19's junket, including in respect of Customer 19 himself as a key player on those junkets: see paragraphs 483ff.

Crown Melbourne and Crown Perth were unable to monitor the ML/TF risks posed by transactions associated with Customer 19's junkets, including transactions by his junket representatives and key players on his junkets, because they did not make and keep appropriate records of designated services provided.

Crown Melbourne did not apply appropriate risk-based transaction monitoring to designated services provided to Customer 19: paragraphs 590ff, 629 to 642 and 643 to 649.

In 2021, an independent auditor identified Customer 19 as responsive to an ML/TF 'risk area' as a result of Customer 19's activity as a junket operator. The independent auditor noted that junkets are high risk for casino ML/TF activity and therefore patrons identified as junket operators, including Customer 19, presented a higher ML/TF risk to Crown Melbourne and Crown Perth.

Transactions indicative of ML/TF typologies – parked funds

Transactions involving Customer 19 were identified as indicative of the ML/TF typology of parked funds. Customer 19's safekeeping account contained $1,690,572 between at least 12 February 2020 and 18 June 2021.

Inadequate controls on Crown's private jets

On 25 August 2016, Crown Melbourne provided Customer 19 with access to a Crown private jet from a foreign country to Perth for two people.

There were inadequate controls on the carrying of large amounts of cash on Crown's private jets: see paragraphs 454 and 491(c).

Ongoing customer due diligence

1190. On and from 1 March 2016, on multiple occasions, the provision of designated services to Customer 19 raised red flags reflective of higher ML/TF risks as a result of:

a. his individual and junket play, which involved high turnover; and

b. his involvement in complex and unusually large transactions and unusual patterns of transactions, often with third parties, which had no apparent economic or visible lawful purpose.

Particulars

See paragraphs 477 and 456ff.

Between 27 March 2016 and 10 April 2016, Customer 19 operated a junket (AUD) at Crown Melbourne with one key player. The key player recorded a loss of $2,400,000: SMR dated 11 April 2016.

On 19 May 2016, Customer 19 received a telegraphic transfer of $1,998,000 into his junket account from a third party who was not a key player in Customer 19's junket: SMR dated 20 May 2016.

On 20 September 2016, Customer 19 transferred $1,489,296 into his Crown Perth DAB account.

On 24 January 2017, Crown Aspinalls informed Crown Resorts that Customer 19 had played at Crown Aspinalls on 30 – 31 July 2016 with a turnover of GBP28,971,000.

By 1 February 2017, Customer 19 had a turnover at Crown Melbourne and Crown Perth of approximately $1,000,000,000.

By 18 July 2017:

- Customer 19's junket had a cumulative turnover at Crown Melbourne of $731,000,000 with a loss of $2,400,000;
- Customer 19 had a cumulative turnover at Crown Perth of $200,000,000 with a loss of $7,800,000;
- Customer 19 had a cumulative turnover at Crown Aspinalls of GBP29,000,000 with a loss of GBP1,400,000; and
- Customer 19 had a credit limit of $10,000,000 at Crown Perth and Crown Melbourne.

By 11 July 2018, Customer 19's cumulative turnover at Crown Melbourne had increased to $899,000,000 with a loss of $3,000,000. Customer 19 had not increased his turnover at Crown Perth or Crown Aspinalls. Customer 19 had a credit limit of $10,000,000 at Crown Perth and Crown Melbourne.

On 18 March 2019, Crown Melbourne, Crown Perth and Customer 19 entered into a NONEGPRA.

By 24 April 2019, Customer 19's cumulative turnover at Crown Melbourne had increased to $1,114,000,000 with a loss of $5,400,000. Customer 19 had not increased his turnover at Crown Perth. Customer 19 had a credit limit of $5,000,000 at Crown Perth and Crown Melbourne.

On 25 September 2019, the Group General Manager (International Business Operations) approved a credit facility for Customer 19 with a credit limit of $3,000,000 in advance of a junket trip commencing that day with one key player, Person 21. The junket was a 30% hybrid program. The credit was subject to the condition that any net winnings in the junket program were to be paid to Crown Aspinalls towards a large debt incurred by a key player and foreign PEP in Customer 19's junket, Person 21, that had been outstanding since 14 January 2010.

As at 7 October 2019, Customer 19 ran four VIP International Programs, being special junket programs requiring commercial and executive approval, together with another customer. Each of the programs offered a 30% rebate on gross win/loss.

As at 17 March 2020, Customer 19's junket program had a cumulative turnover at Crown Melbourne of $1,500,000,000 with a loss of $5,500,000. Customer 19 had not increased his turnover at Crown Perth. Customer 19 had a credit limit of $5,000,000 with a TTO of $15,000,000. Customer 19 had last visited Crown Melbourne on 29 April 2019.

As at 4 January 2021, Customer 19 had an outstanding debt at Crown Melbourne of $9,665,059 that had been due in January 2020 and a DAB account balance of $1,690,572. A number of key players on Customer 19's junket programs had a high turnover. Customer 19 personally had a turnover of $44,800,000 and loss of $6,500,000.

By 5 January 2021, Crown Melbourne were aware that several key players on Customer 19's junket, including Person 21, were foreign PEPs.

1191. At no time did Crown Melbourne or Crown Perth undertake appropriate risk-based customer due diligence with respect to Customer 19 with a view to identifying, mitigating and managing the ML/TF risks posed by the provision of designated services on and from 1 March 2016.

a. At no time did Crown Melbourne take appropriate steps to understand whether Customer 19's source of wealth/funds was legitimate.

b. At no time did Crown Perth take appropriate steps to understand whether Customer 19's source of wealth/funds was legitimate.

c. At no time did Crown Melbourne or Crown Perth take appropriate steps to identify or analyse the ML/TF risks of Customer 19's transactions or to consider whether they had a lawful purpose.

d. At no time did Crown Melbourne and Crown Perth gave any consideration at any time to whether large and high risk transactions should be processed.

e. On each occasion that senior management considered whether to continue the business relationship with Customer 19, senior management failed to give adequate consideration to whether the ML/TF risks posed by Customer 19 were within Crown Melbourne or Crown Perth's risk appetite.

Particulars

Section 36(1)(a) of the Act.

The due diligence steps taken with respect to Customer 19 included:

Database searches

In March 2016, July 2016, December 2016, January 2017, May 2017, February 2018, April 2018, March 2019, September 2019 and January 2021, Crown Melbourne conducted a number of searches in respect of Customer 19 on open source and subscription databases:

- searches in December 2016 revealed that Customer 19 was a foreign PEP by association and identified Customer 19's business interests; and
- a report from January 2021 identified a media article dated 28 June 2010 which said that Customer 19 was a prominent in the 'underworld' of the entertainment industry in a foreign country, was involved in illegal activities including gambling and was involved in gang-related activity.

At no point, as a result of these searches, did Crown Melbourne appropriately consider the ML/TF risks of the source of Customer 19's wealth/funds or whether an ongoing business relationship with Customer 19 was within its ML/TF risk appetite.

There is no evidence of Crown Perth conducting any separate searches in respect of Customer 19.

Wealth information

In April 2016, July 2016, December 2016, February 2018, April 2019, September 2019 and February 2021, Crown Melbourne obtained a wealth report in respect of Customer 19 for the purposes of assessing credit risk.

On 24 September 2019, as part of a request to reactivate a $3,000,000 credit limit at Crown Melbourne, a credit analyst identified Customer 19's net worth and noted that Customer 19 had outstanding balances at several other casinos.

The credit was approved subject to the condition that any net winnings in the junket program were to be paid to Crown Aspinalls towards a large debt incurred by a key player on Customer 19's junket, Person 21, that had been outstanding since 14 January 2010.

The ML/TF risks of approving the credit on this basis were not considered.

There is no evidence of Crown Perth obtaining any separate wealth information in respect of Customer 19.

Junket profile

In July 2017, the Credit control team prepared a junket profile in respect of Customer 19 and his junket operations for the purpose of assessing his creditworthiness. The profile:

- set out Customer 19's credit limit and turnover at Crown Melbourne, Crown Perth and Crown Aspinalls;
- set out Customer 19's junket and individual credit lines at other casinos;
- noted that Customer 19 conducted a junket at another Australian casino which required police clearance; and
- summarised the findings of a number of due diligence searches and wealth reports obtained in respect of Customer 19.

Customer 19's junket profile was updated on July 2018 and April 2019. Each junket profile recommended that Crown Melbourne continue to conduct business with him, but did not provide a basis for this decision.

Crown Melbourne did not appropriately consider the ML/TF risks of the source of Customer 19's wealth/funds in any of the junket profiles.

There is no evidence of Crown Perth separately considering the junket profiles in respect of Customer 19.

Senior management engagement

Senior management considered Crown Melbourne's business relationship with sun on 1 February 2017 at a VIP Operations meeting. The meeting recommended suspending business with Customer 19 until Crown Resorts could establish a domicile outside of a foreign country. This decision was not made on the basis on ML/TF risk.

On 17 July 2017, after Customer 19 had provided documents confirming his domicile, the Group General Manager (International Business Operations) approved a credit limit of $5,000,000 in advance of a trip commencing that evening. There is no evidence that the Group General Manager (International Business Operations) considered the ML/TF risks associated with Crown Melbourne's business relationship with Customer 19 when approving the credit limit. At no point did senior management appropriately consider whether a business relationship with Customer 19 was within Crown Melbourne's ML/TF risk appetite.

There is no evidence that Crown Perth senior management took any separate steps to consider whether Crown Perth's relationship with Customer 19 was within its ML/TF risk appetite.

None of these steps were proportionate to the ML/TF risks reasonably posed by Customer 19 on and from 1 March 2016.

Enhanced customer due diligence

1192. Having formed a suspicion for the purposes of s41 of the Act, Crown Melbourne gave the AUSTRAC CEO SMRs with respect to Customer 19 on:

a. 11 April 2016; and

b. 20 May 2016.

Particulars

The 11 April 2016 SMR reported significant losses noted for key players in Customer 19's junket.

The 20 May 2016 SMR reported a large telegraphic transfer, pleaded at paragraph 1190, received for Customer 19's junket on 19 May 2016 from a third party not listed as a key player in Customer 19's junket.

1193. On each occasion that Crown Melbourne formed a suspicion with respect to Customer 19 for the purposes of s41 of the Act, it was required to apply its ECDD program to Customer 19.

Particulars

Rule 15.9(3) of the Rules.

1194. Crown Melbourne did not carry out appropriate risk-based ECDD measures with respect to Customer 19 on each occasion that Crown Melbourne formed a suspicion with respect to Customer 19 for the purposes of s41 of the Act.

a. There are no records of ECDD being conducted following the lodgement of the SMR on 20 May 2016: see paragraphs 664 and 685.

b. Appropriate risk-based steps were not taken to obtain or analyse information about Customer 19's source of wealth/funds: see paragraph 667.

c. Appropriate risk-based steps were not taken to analyse and monitor Customer 19's transactions – both past and future – including to understand their economic purpose: see paragraph 590 and 666.

d. On each occasion that senior management considered whether to continue the business relationship with Customer 19, senior management failed to give adequate consideration to whether the ML/TF risks posed by Customer 19 were within Crown Melbourne's risk appetite.

Particulars

Rules 15.9(3), 15.10(1)(c), (d), (2), (5) and (6) of the Rules.

In the period immediately prior to giving the 11 April 2016 SMR to the AUSTRAC CEO, Crown Melbourne confirmed Customer 19's business interests, conducted a company search, a risk intelligence search and obtained a wealth report in respect of Customer 19.

On 1 February 2017, senior management determined not to continue a business relationship with Customer 19 until he could establish a

domicile outside of a particular foreign country. Customer 19 had a credit limit of $5,000,000 approved on 17 July 2017 after documentation from a second foreign country was provided to Crown Melbourne, and a business relationship was reinstated.

On 18 July 2017, 11 July 2018, 24 April 2019, Crown Melbourne prepared a junket profile in respect of Customer 19's junket with ultimate recommendation that Crown Melbourne continue to conduct business with Customer 19 despite the high ML/TF risk posed by Customer 19 as pleaded at paragraph 1181 and 1188.

See particulars to paragraph 1191.

1195. At all times from 1 March 2016, Customer 19 was a foreign PEP.

Particulars

Section 36(1)(a) of the Act

Customer 19 was a foreign PEP by family associated with a prominent member of a foreign political party.

1196. At all times from 1 March 2016, Crown Melbourne and Crown Perth was required to apply its ECDD program to Customer 19.

Particulars

Rules 15.9(2) and 15.11 of the Rules

1197. Crown Melbourne and Crown Perth did not carry out appropriate risk-based ECDD measures with respect to Customer 19 on and from 1 March 2016 given his status as a foreign PEP. In particular:

a. Crown Melbourne and Crown Perth did not undertake a detailed analysis of Customer 19's KYC information or analyse the legitimacy of Customer 19's source of wealth/funds;

b. no adequate steps were taken to seek and obtain senior management approval for continuing a business relationship with Customer 19 having regard to the ML/TF risks posed by the customer. Decisions made by senior management to continue a business relationship did not consider, and were not made in relation to, Customer 19's status as a foreign PEP; and

c. no adequate steps were taken to seek and obtain senior management approval for whether Crown Melbourne should continue to provide designated services to Customer 19. Decisions made by senior management to continue a business relationship did not consider, and were not made in relation to, Customer 19's status as a foreign PEP.

Particulars

Rules 15.10(2), 15.10(6), 15.11 of the Rules.

See particulars to paragraph 1191.

See paragraph 660, 663, 666, 667 and 668.

1198. By reason of the matters pleaded from paragraphs 1175 to 1197, on and from 1 March 2016, Crown Melbourne and Crown Perth:

a. did not monitor Customer 19 in relation to the provision of designated services, with a view to identifying, mitigating and managing the ML/TF risks it reasonably faced; and

b. did not do so in accordance with rr 15.5 and 15.9 of the Rules.

1199. By reason of the matters pleaded at paragraph 1198, Crown Melbourne and Crown Perth contravened s36(1) of the Act on and from 1 March 2016 with respect to Customer 19.

Particulars

Section 36(1) of the Act is a civil penalty provision: s36(2) of the Act.

INTERNATIONAL CUSTOMERS

Customer 20

1200. Customer 20 has been a customer of Crown Melbourne since 6 August 2015.

1201. Between at least August 2015 and 22 January 2021, Crown Melbourne provided Customer 20 with designated services within the meaning of table 1 and table 3, s6 of the Act.

Particulars

On 6 August 2015, Crown Melbourne opened a DAB account and safekeeping account (AUD) for Customer 20, which remain open.

Crown Melbourne recorded Customer 20's individual rated gaming activity between 2016 and 2019 to be a cumulative loss of $747,020.

On 22 January 2021, Crown Melbourne issued a WOL in respect of Customer 20.

1202. From at least August 2015 and 2019, Customer 20 received designated services as a junket player, facilitated through two different junket operators.

Particulars

Customer 20 received designated services through the Suncity and Neptune junkets.

Between 6 August 2015 and 15 July 2019, Customer 20 attended 41 junket programs.

Crown Melbourne recorded Customer 20's junket activity in 2015 to be a cumulative turnover of $274,154,720 with a cumulative win of $2,275,990.

Crown Melbourne recorded Customer 20's junket activity between 2016 and 2019 to be a cumulative turnover of $1,127,385,731 with a cumulative win of $3,326,676.

The ML/TF risks posed by Customer 20

1203. By 1 March 2016, higher ML/TF risks were indicated by the nature and purpose of Customer 20's business relationship with Crown Melbourne, the nature of the transactions he

had been conducting, together with the suspicions Crown Melbourne itself had formed with respect to Customer 20.

Particulars

Section 36(1)(a), (b) of the Act and Chapter 15 of the Rules.

Customer 20 was a junket player. He received designated services through the channel of junket programs. This channel lacked transparency: see paragraph 477.

By 1 March 2016, Crown Melbourne had given the AUSTRAC CEO two SMRs in relation to Customer 20 – on 1 September 2015 and 23 September 2015. Each SMR reported the same repeated patterns of suspicions relating to losses under a junket program and the amount of cash Customer 20 was prepared to carry. The 23 September 2015 SMR identified a suspicion that a junket representative had exchanged $500,000 in gaming chips for cash on behalf of Customer 20, who already had $1,000,000 in cash in his possession.

As at 1 March 2016, Customer 20 had played in eight junket programs with a cumulative turnover of $274,150,000 with a cumulative win of $2,272,510.

As at 1 March 2016, no due diligence steps were taken with respect to Customer 20.

1204. By November 2016, Customer 20 should have been recognised by Crown Melbourne as a high risk customer for the reasons pleaded at paragraphs 1203, 1207, 1208, 1209, 1210, 1211 and 1214.

1205. At all times on and from November 2016, Customer 20 should have been recognised by Crown Melbourne as a high risk customer by reason of the matters pleaded at paragraphs 1203, 1207, 1208, 1209, 1210, 1211, 1212 and 1214.

Particulars

Section 36(1)(a), (b) of the Act and Chapter 15 of the Rules.

1206. It was not until 29 May 2019 that Crown Melbourne rated Customer 20's risk as high.

Particulars

On various occasions between 1 September 2015 and 8 January 2018, Crown Melbourne rated Customer 20's risk as moderate.

In November 2016, Crown Melbourne exchanged $250,000 in $50 notes to $100 notes at the request of Customer 20. This transaction was indicative of the ML/TF typology of refining. Coupled with Customer 20's significant junket activity and the many international third party transactions sent and received by Customer 20, this should have alerted Crown Melbourne to the high ML/TF risk posed by Customer 20.

On various occasions between 9 January 2018 and 28 May 2019, Crown Melbourne rated Customer 20's risk as significant.

On 29 May 2019, in response to a law enforcement inquiry received by Crown Melbourne in respect of Customer 20, Crown Melbourne rated Customer 20's risk as high for the first time. On various occasions between 29 May 2019 and 20 January 2021, Crown Melbourne rated Customer 20's risk as high.

See paragraph 481.

1207. On and from 1 March 2016 designated services provided to Customer 20 posed higher ML/TF risks including because the provision of designated services to Customer 20 involved a combination of the following factors:

a. Customer 20 was a junket player;

b. Customer 20 received large value financial (table 1, s6) and gaming services (table 3, s6) provided through multiple junket programs;

c. by no later than 15 July 2019, Customer 20's cumulative junket turnover exceeded $1,400,000,000;

d. Customer 20 was known at all times to be connected to the junket operator of the Suncity junket, Customer 1, in respect of whom Crown Melbourne had formed suspicions: see paragraph 521ff;

e. Customer 20 was involved in regular and substantial transactions with the junket operator of the Suncity junket: see paragraph 521ff;

f. designated services provided to Customer 20 involved a lack of transparency as the services were provided through the channel of junket programs;

g. Customer 20 transacted with large and suspicious cash, including large volumes of cash in small notes in a brown paper bag with writing on the side, in shopping bags and in a suitcase;

h. on multiple occasions, Customer 20 deposited or exchanged large and suspicious cash comprising bundled $50 notes;

i. in November 2016, Customer 20 exchanged $250,000 in cash comprising bundled $50 notes for $100 notes with no associated gaming activity. This transaction was indicative of the ML/TF typology of refining;

j. designated services provided to Customer 20 involved large transfers to and from third parties, including to and from a junket operator and unknown third parties: see paragraph 456ff;

k. between April 2016 and February 2018, Customer 20 received at least $3,943,000 from, and sent at least $742,000 to, a third party, Person 16. Between October 2016 and June 2019, Customer 1, received at least $2,000,000 from, and sent at least $4,956,000 to, Person 16 on Customer 20's behalf;

l. in May 2019, Customer 1, on Customer 20's behalf, received into his Crown Melbourne DAB account three telegraphic transfers totalling $2,000,000 from a foreign third party with reference 'Payment to Supplier'. While Crown Melbourne ultimately refused the third of these transactions, they nonetheless accepted a further transaction from the same third party of $693,000 in June 2019;

m. designated services provided to Customer 20 involved large cross-border movements of funds: see paragraph 238(d);

n. large values of funds were transferred to and from Customer 20's bank accounts and his DAB account, and to and from other customers' DAB accounts, involving designated services within the meaning of items 31 and 32, table 1, s6 of the Act;

o. these transactions took place against the background of:

   i. two SMRs being given to the AUSTRAC CEO by Crown Melbourne by 1 March 2016;

   ii. in 2015, a high cumulative junket turnover of $274,154,720; and

   iii. in September 2015, large and suspicious cash transactions completed by junket representatives on Customer 20's behalf;

p. between January 2018 and May 2019, Customer 20 was the subject of law enforcement inquiries on four occasions. At least one inquiry related to dealing with property reasonably suspected of being proceeds of crime; and

q. by reason of the matters set out at subparagraphs a. to p. above, there were real risks that Customer 20's source of wealth and source of funds were not legitimate.

Monitoring of Customer 20's transactions

1208. At no time did Crown Melbourne appropriately monitor Customer 20's transactions on a risk-basis.

Particulars

Section 36(1)(a), (b) of the Act and rules 15.4 to 15.8 of the Rules.

Crown Melbourne was unable to monitor the ML/TF risks posed by Customer 20's transactions appropriately because it did not make and keep appropriate records of designated services provided to junket players: see paragraphs 483ff.

Crown Melbourne did not apply appropriate risk-based transaction monitoring to designated services provided to Customer 20: see paragraphs 590ff, 629 to 642 and 643 to 649.

Customer 20's transactions involved repeated transactions indicative of ML/TF typologies and vulnerabilities that were not detected. Had appropriate risk-based transaction monitoring been applied, these transactions could have been identified earlier: see paragraphs 686 and 687.

On 6 November 2016, for reasons suspected by Crown Melbourne to be other than for gaming purposes, Crown Melbourne exchanged for the Suncity junket $250,000 in $50 notes to $100 notes. The cash was believed to belong to Customer 20: SMR dated 7 November 2016. The transaction was indicative of the ML/TF typology of refining.

Ongoing customer due diligence

1209. On and from 1 March 2016, on multiple occasions, the provision of designated services to Customer 20 raised red flags reflective of higher ML/TF risks as a result of Customer 20's frequent, large transactions with a number of third parties including repeated transactions with Customer 1 and a third party, Person 16.

Particulars

See paragraphs 456ff and 477.

Third party transactions in 2016

On 1 April 2016, Customer 20 received into his Crown Melbourne DAB account an international telegraphic transfer from a third party: SMR dated 4 April 2016. The funds appear to have been used as front money on a junket program.

On 20 and 21 April 2016, Customer 20 received into his Crown Melbourne DAB account two international telegraphic transfers totalling $410,000 from a third party: SMR dated 22 April 2016.

On 6 May 2016, Customer 20 received into his Crown Melbourne DAB account an international telegraphic transfer of $463,000 from a third party: SMR dated 6 May 2016.

On 15 July 2016, while playing on a Suncity junket program Customer 20 requested that Customer 1 send $50,000 by international telegraphic transfer to a third party, Person 43: SMR dated 18 July 2016.

On 5 October 2016, Customer 20 received into his Crown Melbourne DAB account a telegraphic transfer of $480,000 from Person 16 which was then transferred to Customer 1's Crown Melbourne DAB account. Customer 20 was playing under a Suncity junket program at the time. The funds were used to repay a debt owed by Customer 20 to Crown Melbourne.

On 7 October 2016, Customer 20 received into his Crown Melbourne DAB account a telegraphic transfer of $520,000 from Person 16 with reference 'Front Money banked'.

On 23 October 2016, while Customer 20 was playing on a Suncity junket, Customer 1 transferred from his Crown Melbourne DAB account $70,000 to Person 16. This appears to have been on Customer 20's behalf.

On 14 November 2016, 28 November 2016, 14 December 2016 and 12 January 2017, Customer 1 transferred from his Crown Perth DAB account $83,000, $350,000, $120,000 and $116,000 respectively to Person 16. This appears to have been on Customer 20's behalf. Customer 20 was playing on a Suncity junket at Crown Melbourne at the time.

Third party transactions in 2017

On 19 January 2017, Customer 20 received into his Crown Melbourne DAB account a telegraphic transfer of $500,000 from Person 16.

On 24 February 2017, while showing a win of $293,225 on a Suncity junket program, Customer 20 requested that Customer 1 transfer from his Crown Melbourne DAB account $100,000 to a third party: SMR dated 27 February 2017.

On 15 March 2017, Customer 20 requested Customer 1 from his Crown Melbourne DAB account transfer $50,000 to a third party, Person 43: SMR dated 17 March 2017. Customer 20 was playing on a Suncity junket at Crown Melbourne at the time.

On 21 April 2017, Customer 20 received into his Crown Melbourne DAB account a telegraphic transfer from Person 16 of $500,000.

On 31 May 2017 and 14 June 2017, Customer 1 transferred from his Crown Melbourne DAB account $220,000 and $167,000 respectively to Person 16. This appears to have been on Customer 20's behalf. Customer 20 was playing on a Suncity junket at Crown Melbourne at the time.

On 10 July 2017, Customer 20 sent from his Crown Melbourne DAB account a telegraphic transfer to Person 16 of $112,000.

On 29 November 2017, Customer 20 received into his Crown Melbourne DAB account a telegraphic transfer of $893,000 from Person 16 which he then transferred to Customer 1: SMR dated 1 December 2017. Customer 20 was playing on the Suncity junket at Crown Melbourne at the time.

Third party transactions in 2018

On 16 January 2018, Customer 20 requested that Customer 1 send a telegraphic transfer from his Crown Melbourne DAB account to a third party, Person 43: SMR dated 17 January 2018. Customer 20 was playing on the Suncity junket at Crown Melbourne at the time.

On 10 February 2018, Customer 20 received into his Crown Melbourne DAB account a telegraphic transfer of $850,000 from Person 16: SMR dated 12 February 2018.

On 15 March 2018, 18 April 2018, 8 May 2018, 25 June 2018, and 30 August 2018, Customer 1 transferred from his Crown Melbourne DAB account $800,000, $300,000, $800,000, $880,000 and $950,000 respectively Person 16. This appears to have been on Customer 20's behalf. Customer 20 was playing on the Suncity junket at Crown Melbourne at the time.

Third party transactions in 2019

On 26 January 2019, Customer 20 sent from his Crown Melbourne DAB account a telegraphic transfer to Person 16 of $630,000.

On 24 May 2019, Customer 1 received into his Crown Melbourne DAB account two telegraphic transfers of $650,000 and $657,000 respectively from Person 16 with reference 'Payment to Supplier'. The funds were for Customer 20. Customer 20 was playing on a Suncity junket at Crown Melbourne at the time. Crown Melbourne requested that Person 16 provide a letter stating that the funds were for gaming services, until which time the telegraphic transfers were not accepted by Crown Melbourne. Customer 1 was not asked to provide a similar letter. On 28 May 2019, a third telegraphic transfer of $693,000 was received into his Crown Melbourne DAB account from Person 16 into Customer 1's account with the same reference. The funds were returned to the third party: SMRs dated 24 May 2019 and 28 May 2019.

On 5 June 2019, Customer 1 received into his Crown Melbourne DAB account a telegraphic transfer of $693,000 from Person 16. The funds were believed to be for Customer 20: SMR dated 6 June 2019. Customer 20 was not playing on a Suncity junket at Crown Melbourne at the time that Customer 1 received the transfer.

This is the last recorded transaction to or from Person 16. In total, between 4 April 2016 and 12 February 2018, Customer 20 received at least $3,943,000 across 7 transactions from Person 16, and Customer 20 sent at least $742,000 across 2 transactions to Person 16. In total, between 23 October 2016 and 5 June 2019, Customer 1 received at least $2,000,000 across 3 transactions from Person 16 and Customer 1 sent at least $4,956,000 across 13 transactions to Person 16 on behalf of Customer 20.

On 14 July 2019, Customer 1 transferred from his Crown Melbourne DAB account $600,000 to Customer 20's personal account. Customer 20 was playing on a Suncity junket at Crown Melbourne at the time.

1210. On and from 1 March 2016, on multiple occasions, the provision of designated services to Customer 20 raised red flags reflective of higher ML/TF risks as a result of:

a. complex, unusually large transactions and unusual patterns of transactions involving Customer 20 which had no apparent economic or visible lawful purpose; and

b. transactions involving large amounts of cash and cash that appeared suspicious.

Particulars

See paragraphs 450, 451 and 491.

Unusual transactions and patterns of transactions in 2016

On 17 July 2016, Customer 20 transferred $100,000 from his Crown Melbourne DAB account to Customer 1.

Unusual transactions and patterns of transactions in 2017

On 24 November 2017, while showing a loss of $1,500,000 under a junket program, Customer 20 presented at the Suncity cash administration desk with two shopping bags containing approximately

$300,000 in $100 notes which he exchanged for gaming chips. Crown Melbourne staff observed the transaction from a distance and so the exact amount of the transaction was unknown. Customer 20 did not play at the gaming salon after the transaction: SMR dated 24 November 2017.

On 24 November 2017, while Customer 20 was a key player in a junket program, an unknown person known to be associated with Customer 20 deposited approximately $20,000 in cash at the Suncity cash administration desk but did not play: SMR dated 27 November 2017.

On 22 December 2017, while a key player in a junket program, Customer 20 was observed exchanging $700,000 of cash for chips at the Suncity cash administration desk and then proceeding to use the chips for gaming services: SMR dated 22 December 2017.

Unusual transactions and patterns of transactions in 2018

On 5 January 2018, Customer 20 was observed depositing approximately $500,000 in $50 bundled notes packed in a suitcase at the Suncity cash administration desk. Customer 20 proceeded to use gaming services for a very short period of time and then deposited a further amount of approximately $800,000: SMR dated 9 January 2018. Initially, Crown Melbourne was not able to identify the individual who made the deposit. However, the Vice President (International Business Operations) identified Customer 20 after seeing an image and noted that he regularly would cash out his winnings during a junket program and then redeposit the cash.

On 10 January 2018, while showing a win under a junket program of $100,000, Customer 20 presented to the Suncity cash administration desk with a suitcase containing $155,000 in cash for deposit: SMR dated 11 January 2018.

On 16 January 2018, Customer 20 presented at the Suncity cash administration desk with $120,000 in cash to buy-in for gaming purposes.

On 8 February 2018, Customer 20 presented at the Suncity cash administration desk with approximately $800,000 in cash contained in a brown paper bag with white writing on the side covered in a black t-shirt. Customer 20 deposited $400,000 in cash at the Suncity cash administration desk and retained $400,000: SMR dated 9 February 2018.

On 7 March 2018, Customer 20 was showing a win of $2,410,000 during a Suncity junket program. A representative for the Suncity junket withdrew $1,910,000 from Customer 1's DAB account. The junket representative advised Crown Melbourne that Customer 20 intended to take his funds in cash rather than sending telegraphic transfers, and that while Customer 20 was not immediately leaving the country he wished "to have the cash ready at any time": SMR dated 8 March 2018.

Unusual transactions and patterns of transactions in 2019 and 2020

Between 16 December 2019 and 2 January 2020, Customer 20 transferred from his personal account approximately $1,100,000 to Customer 1 in units of $100,000. However, Customer 20 was not a key player on a Suncity junket at Crown Melbourne at the time.

The last junket program in which Customer 20 was a key player was in July 2019: SMRs dated 27 December 2019, 31 December 2019, 2 January 2020, 3 January 2020. Customer 20 was due to attend Crown Melbourne on a Suncity junket program on 22 January 2020 but had postponed his trip until further notice with the funds to remain with the junket.

1211. On and from 1 March 2016, on multiple occasions, the provision of designated services to Customer 20 raised red flags reflective of higher ML/TF risks as a result of Customer 20's junket activity.

Particulars

See paragraph 477.

In 2016, Crown Melbourne recorded that Customer 20 had a cumulative junket turnover of $368,821,175 with a cumulative loss of $6,370,895. Customer 20 had a cumulative individual rated gaming activity loss of $1,918,230.

In 2017, Crown Melbourne recorded that Customer 20 had a cumulative junket turnover of $297,939,845 with a cumulative loss of $1,063,205. Customer 20 had a cumulative individual rated gaming activity win of $1,173,210.

In 2018, Crown Melbourne recorded that Customer 20 had a cumulative junket turnover of $419,898,020 with a cumulative win of $8,539,760.

In 2019, Crown Melbourne recorded that Customer 20 had a cumulative junket turnover of $40,726,690 with a cumulative win of $2,221,016.

1212. On and from 1 March 2016, on multiple occasions, the provision of designated services to Customer 20 raised red flags reflective of higher ML/TF risks as a result of receiving numerous inquiries from law enforcement agencies in respect of Customer 20.

Particulars

On 10 January 2018, Crown Melbourne received a law enforcement inquiry in respect of Customer 20. The law enforcement agency requested footage of the two deposits made by Customer 20 of $500,000 and $800,000 together with other persons, such as the junket operator, or vehicles associated with him. The request was made in connection with Customer 20's dealing with property reasonably suspected of being proceeds of crime.

Crown Melbourne also received law enforcement inquiries in respect of Customer 20 on 17 January 2018, 18 January 2018, 28 February 2018 and 24 May 2019.

1213. At no time did Crown Melbourne undertake appropriate risk-based customer due diligence with respect to Customer 20 with a view to identifying, mitigating and managing the ML/TF risks posed by the provision of designated services on and from 1 March 2016.

a. At no time did Crown Melbourne take appropriate steps to understand whether Customer 20's source of wealth/funds was legitimate.

b. At no time did Crown Melbourne take appropriate steps to identify or analyse the ML/TF risks of Customer 20's transactions or to consider whether they had a lawful purpose.

c. With the exception of three telegraphic transfers received for Customer 20 in May 2019 from Person 16, Crown Melbourne gave no consideration at any time to whether large and high risk transactions should be processed. In May 2019, Crown Melbourne refused to accept two telegraphic transfers until a signed letter stated that the funds were for gaming purposes because the reference for those transfers was 'Payment to Supplier'. A third telegraphic transfer was returned for the same reason. Nonetheless, in June 2019, Crown Melbourne accepted a telegraphic transfer from the same third party.

d. Prior to the decision to issue Customer 20 with a WOL in January 2021, there is no record of senior management considering whether continuing the business relationship with Customer 20 was within Crown Melbourne's ML/TF risk appetite in light of the ML/TF risks posed by Customer 20.

Particulars

Section 36(1)(a) of the Act.

The due diligence steps taken with respect to Customer 20 included:

Wealth and risk intelligence reports

In December 2016, Crown Melbourne obtained a wealth report in respect of Customer 20 which did not reveal any information about his source of wealth/funds.

In January 2018, Crown Aspinalls provided their due diligence file in respect of Customer 20, which contained a risk intelligence report.

At no point, as a result of these reports, did Crown Melbourne appropriately consider the ML/TF risks of the source of Customer 20's wealth/funds or whether an ongoing business relationship with Customer 19 was within its ML/TF risk appetite.

Database searches

In December 2016, May 2019, November 2019, December 2019 and March 2020, Crown Melbourne conducted a risk intelligence search in respect of Customer 20.

In March 2020, Crown Melbourne conducted open source media searches in respect of Customer 20.

At no point, as a result of these searches, did Crown Melbourne appropriately consider the ML/TF risks of the source of

Customer 20's wealth/funds or whether an ongoing business relationship with Customer 20 was within its ML/TF risk appetite.

Transaction monitoring

As pleaded at the particulars to paragraph 1209, in May 2019 Customer 1 received three telegraphic transfers on Customer 20's behalf from an international third party, Person 16, with reference 'Payment to Supplier'. Crown Melbourne had on file the third party's foreign driver's licence. The Senior Vice President (International Business) suggested that Crown Melbourne ask Person 16 to sign a standard letter confirming that the transactions were for gaming purposes, which he did. The Group General Manager (AML) requested that a report be prepared in respect of Person 16. Crown Melbourne conducted a risk intelligence search in respect of Person 16.

Crown Melbourne did not give appropriate consideration to whether large and high risk transactions should be processed and did not appropriately consider the ML/TF risks of transactions between Customer 20, Customer 1 and Person 16. Moreover, in June 2019, Crown Melbourne accepted a telegraphic transfer from the same third party.

Senior management engagement

On 11 January 2018, the CTRM noted that there were no wealth reports or risk intelligence reports in respect of Customer 20.

As pleaded at the particulars to paragraph 1210, on 5 January 2018 and 8 February 2018 Customer 20 engaged in suspicious large cash transactions at the Suncity cash administration desk involving over $2,000,000, $1,700,000 of which was deposited. Other than the investigative steps described above, Crown Melbourne did not take further steps to inquire into the source, or legitimacy of the source, of Customer 20's funds.

In March 2020, the AML Manager asked the Senior Vice President (International Business Operations) whether information was known about Customer 20's occupation, business and position with his business, source of wealth and source of funds. By this time, Customer 20 had a cumulative junket turnover at Crown Melbourne of $1,401,540,451.

Senior management failed to consider whether a business relationship with Customer 20 was within Crown Melbourne's ML/TF risk appetite

None of these steps were proportionate to the ML/TF risks reasonably posed by Customer 20 on and from 1 March 2016.

In January 2021, a Group POI Committee meeting was held. The POI Committee decided to issue a WOL in respect of Customer 20, noting the ILGA inquiry.

Customer 20 was issued with a WOL on 22 January 2021.

Enhanced customer due diligence

1214. Having formed a suspicion for the purposes of s41 of the Act, Crown Melbourne gave the AUSTRAC CEO 27 SMRs with respect to Customer 20: Schedule 3.7.

Particulars

These SMRs reported third party transfers and in particular the transfer with reference 'Payment to Supplier', annual individual and junket losses, exchanges of cash not believed to be for gaming purposes, funds presented for deposit at the Suncity cash administration desk with and without subsequent play, large cash withdrawals by a junket representative on Customer 20's behalf, transfers by Customer 20 to a junket operator while not a key player in that junket and the amount of cash Customer 20 was prepared to carry.

1215. On each occasion that Crown Melbourne formed a suspicion with respect to Customer 20 for the purposes of s41 of the Act, it was required to apply its ECDD program to Customer 20.

Particulars

Rule 15.9(3) of the Rules.

1216. Crown Melbourne did not carry out appropriate risk-based ECDD measures with respect to Customer 20 on each occasion that Crown Melbourne formed a suspicion with respect to Customer 20 for the purposes of s41 of the Act.

a. Other than following the lodgement of the 9 January 2018, 27 December 2019, 31 December 2019, 2 January 2020 and 3 January 2020 SMRs, there are no records of ECDD being conducted following the lodgement of any SMR: see paragraphs 664 and 685.

b. Appropriate risk-based steps were not taken to obtain or analyse information about Customer 20's source of wealth/funds: see paragraph 667.

c. Appropriate risk-based steps were not taken to analyse and monitor Customer 20's transactions – both past and future – including to understand their economic purpose: see paragraph 590 and 666.

d. Prior to the decision to issue Customer 20 with a WOL in January 2021, there is no record of senior management considering whether continuing the business relationship with Customer 20 was within Crown Melbourne's ML/TF risk appetite in light of the ML/TF risks posed by Customer 20.

Particulars

Rules 15.9(3), 15.10(1)(c), (d), (2), (5) and (6) of the Rules.

ECDD conducted in January 2018

Following the lodgement of the 9 January 2018 SMR, Crown Melbourne conducted due diligence searches in respect of Customer 20. The CTRM asked Crown Melbourne employees for information about Customer 20. In response:

- a Surveillance Analyst provided Customer 20's personal details and identified that no suspicious behaviours had been observed in respect of Customer 20's table play. The Analyst identified three suspicious transactions despite the 16 SMRs filed prior to January 2018, being the transactions the subject of the 23 September 2015, 24 November 2017 and 21 December 2017 SMRs; and
- the Vice President (International Business Operations) stated that Customer 20 came from a wealthy family in a foreign country, played mainly in Australia and another foreign country and was "private about his affairs and little else is known".

No further action was taken.

ECDD conducted in January 2020

After giving the AUSTRAC CEO an SMR on 27 December 2019, 31 December 2019, 2 January 2020 and 3 January 2020 SMRs, Crown Melbourne conducted risk intelligence searches in respect of Customer 20, which returned no results.

Following a meeting between the AML Manager, the Senior Vice President (International Business), General Manager Commercial (VIP International) and the Senior Vice President (International Business Operations), Crown Melbourne senior management decided that they would ask Customer 20 when he next intended to play in the Suncity junket. Customer 20 was due to attend Crown Melbourne as a junket player in January 2020 but postponed his trip and intended to leave the funds transferred to the junket operator in that account.

1217. On and from 29 May 2019, Crown Melbourne rated Customer 20 high risk.

Particulars

Crown Melbourne rated Customer 20 high risk on seven occasions on and from 29 May 2019: see paragraph 1206.

1218. On each occasion that Crown Melbourne rated Customer 20 high risk, Crown Melbourne was required to apply its ECDD program to Customer 20.

Particulars

Rule 15.9(1) of the Rules.

See paragraph 661.

1219. Crown Melbourne did not carry out appropriate risk-based ECDD measures with respect to Customer 20 on each occasion that Crown Melbourne rated Customer 20 high risk.

Particulars

See particulars to paragraph 1216.

See paragraphs 661, 666, 667 and 668.

1220. By reason of the matters pleaded from paragraphs 1200 to 1219, on and from 1 March 2016, Crown Melbourne:

a. did not monitor Customer 20 in relation to the provision of designated services, with a view to identifying, mitigating and managing the ML/TF risks it reasonably faced; and

b. did not do so in accordance with rr 15.5 and 15.9 of the Rules.

1221. By reason of the matters pleaded at paragraph 1220, Crown Melbourne contravened s36(1) of the Act on and from 1 March 2016 to January 2021 with respect to Customer 20.

Particulars

Section 36(1) of the Act is a civil penalty provision: s36(2) of the Act.

Customer 21

1222. Customer 21 has been a customer of Crown Melbourne since August 2000.

1223. From at least December 2006, Crown Melbourne provided Customer 21 with designated services within the meaning of table 1 and table 3, s6 of the Act.

Particulars

On 3 August 2000, Crown Melbourne opened a DAB account and safekeeping account (AUD) for Customer 21, which remain open.

On 17 February 2007, Crown Melbourne approved a credit facility (AUD) for Customer 21, which was closed on 14 July 2017.

Between 2007 and 2015, Crown Melbourne recorded Customer 21's individual rated gaming activity to be a cumulative loss of $137,694,968.

Between 2016 and 2018, Crown Melbourne recorded Customer 21's individual rated gaming activity to be a cumulative loss of $5,353,138.

1224. From at least March 2016, Customer 21 received designated services as a junket player through his pseudonym and pseudonym PID, facilitated through at least one junket operators at Crown Melbourne.

Particulars

By 8 July 2014, Customer 21 was assigned a pseudonym and pseudonym PID that was linked to his primary PID: see paragraphs 680(e) and 1230.

From at least March 2016, Customer 21 was a key player in Customer 2's junket under his pseudonym and pseudonym PID for at least 55 days.

Between 29 June 2018 and 29 August 2018, Customer 21 was a key player in Customer 2's junket under his pseudonym and pseudonym PID with an estimated turnover of $183,334,795.

The ML/TF risks posed by Customer 21

1225. By 1 March 2016, higher ML/TF risks were indicated by the nature and purpose of Customer 21's business relationship with Crown Melbourne, the nature of the transactions he

had been conducting, together with the suspicions Crown Melbourne itself had formed with respect to Customer 21.

Particulars

Section 36(1)(a), (b) of the Act and Chapter 15 of the Rules.

SMRs by 1 March 2016

By 1 March 2016, Crown Melbourne had given the AUSTRAC CEO 28 SMRs in relation to Customer 21 – on 8 November 2006, 14 November 2006, 24 January 2007, 27 February 2007, 27 June 2007, 8 August 2007, 12 October 2007, 16 November 2007, 27 November 2007, 18 December 2007, 14 February 2008, 29 February 2008, 24 April 2008, 28 May 2008, 6 August 2008, 13 August 2008, 20 August 2008, 29 September 2008, 13 March 2009, 12 May 2009, 10 November 2009, 12 November 2009, 19 November 2009, 11 February 2010, 23 August 2010, 12 August 2011, 11 May 2012 and 31 January 2014. The SMRs described Customer 21's annual wins/losses, increase in rated play and average bets, transfers between accounts and to third parties (including his wife) and the amount of cash Customer 21 was prepared to carry.

Third party transfers by 1 March 2016

Between 3 September 2007 and 13 March 2009, on multiple occasions, Customer 21 sent telegraphic transfers to his wife totalling $20,500,000. From May 2008, Crown Melbourne suspected that Customer 21 was using his Crown Melbourne DAB as a clearing system to send funds to his wife rather than sending funds directly from his personal account to her personal account:

- $1,500,000 on 3 September 2007: SMR dated 28 May 2008;
- $2,000,000 on 28 September 2008: SMR dated 28 May 2008;
- $2,000,000 on 30 September 2007: SMR dated 28 May 2008;
- $1,000,000 on 9 October 2007: SMR dated 28 May 2008;
- $2,000,000 on 31 March 2008: SMR dated 24 April 2008;
- $2,000,000 on 22 May 2008: SMR dated 28 May 2008;
- $4,000,000 on 26 September 2008: SMR dated 29 September 2008;
- $1,000,000 on 26 November 2008: SMR dated 13 March 2009; and
- $5,000,000 on 6 November 2008: SMR dated 13 March 2009.

On 5 August 2008, Customer 21 sent a telegraphic transfer of $200,000 to a third party. Earlier that day, Customer 21 had received a $200,000 transfer from another Crown Melbourne patron with the same last name as the third party: SMR dated 6 August 2008.

By 11 February 2010, Customer 21 had received six large telegraphic transfers in a foreign currency. On 11 February 2010, Customer 21 sent a large telegraphic transfer in a foreign currency to a foreign third party and a further large sum in a foreign currency to a foreign third party company. Crown Melbourne suspected that, in part, these funds were not for gaming purposes: SMR dated 11 February 2010.

On the following days, Customer 21 received telegraphic transfers from a foreign third party company, Company 14, into a Southbank account totalling $6,581,473.15. This third party company had also sent substantial telegraphic transfers to the junket operator Customer 4. These transactions were indicative of the ML/TF typology of cuckoo smurfing:

- on 11 August 2011, transfer of $1,000,000: SMR dated 12 August 2011;
- on 14 November 2013, transfer of $1,388,888.90;
- on 21 November 2013, transfer of $1,393,242.75;
- on 21 November 2013, transfer of $1,388,406.80; and
- on 3 December 2013, transfer of $1,410,934.70.

On 31 January 2014, Customer 21 sent a telegraphic transfer of $35,000 to a foreign third party: SMR dated 31 January 2014.

Large and suspicious transactions by 1 March 2016

On 14 February 2008, Customer 21 received a transfer of $100,000 into his Crown Melbourne DAB account from another Crown Melbourne patron: SMR dated 29 February 2008.

On 17 May 2008, Customer 21 received a transfer into his Crown Melbourne DAB account of $200,000 from another Crown Melbourne patron: SMR dated 28 May 2008.

On 5 August 2008, Customer 21 transferred $200,000 from his DAB account to another Crown Melbourne patron: SMR dated 6 August 2008.

On 26 September 2008, Customer 21 transferred $1,700,000 from his DAB account to another Crown Melbourne patron: SMR dated 29 September 2008.

On 11 May 2009, another Crown Melbourne patron deposited a bank cheque for $2,300,000 into his DAB account. The patron then transferred the funds to Customer 21: SMR dated 12 May 2009.

On 16 July 2009, Customer 21 made a cash withdrawal of $117,000: SMR dated 10 November 2009.

On 11 November 2009, another Crown Melbourne patron transferred $2,000,000 from his DAB account to Customer 21: SMR dated 12 November 2009.

On 19 November 2009, another Crown Melbourne patron deposited a bank cheque for $600,000 into his DAB account. The patron then transferred the funds to Customer 21: SMR dated 19 November 2009.

On 11 February 2010, Customer 21 had a DAB account balance of $3,301,186: SMR dated 11 February 2010.

On 21 April 2012, Customer 21 transferred $300,000 from his DAB account to another Crown Melbourne patron: SMR dated 11 May 2012.

Between 2007 and 2015, Crown Melbourne recorded Customer 21's individual rated gaming activity to be a cumulative loss of $137,694,968.

Other red flags

By 8 July 2014, Customer 21 was assigned a pseudonym and pseudonym PID that was linked to his primary PID: see paragraphs 680(e) and 1230.

Customer 21 requested that a pseudonym PID be created for privacy reasons and in order to prevent the recording of his gaming activity in connection with his name.

Due diligence conducted by 1 March 2016

By 1 March 2016, the due diligence steps taken with respect to Customer 21 included obtaining a wealth report in respect of Customer 21, which identified his business interests and high net worth and source of wealth/funds together with his membership of a several foreign political bodies. Despite this, at no point did Crown Melbourne identify Customer 21 to be a foreign PEP.

1226. As at 1 March 2016, Customer 21 should have been recognised by Crown Melbourne as a high risk customer for the reasons pleaded at paragraph 1225.

Particulars

Section 36(1)(a), (b) of the Act and Chapter 15 of the Rules.

1227. At no time was Customer 21 rated high risk by Crown Melbourne.

Particulars

On various occasions between 27 June 2007 and 7 August 2019, Crown Melbourne assessed Customer 21 as moderate risk.

On 27 June 2007, Crown Melbourne assessed Customer 21's pseudonym as moderate risk based on annual losses and an increase in average bet.

At no time was Customer 21 rated high risk by Crown Melbourne. This was despite that, by 1 March 2016:

- Crown Melbourne had given the AUSTRAC CEO 28 SMRs in respect of Customer 21;

- Customer 21's high individual losses and the numerous large and suspicious transactions involving Customer 21 and third parties between 2007 and 2014, including transactions that Crown Melbourne itself suspected were not for gaming purposes; and
- Customer 21 requested that a pseudonym PID be created for privacy reasons and in order to prevent the recording of his gaming activity in connection with his name.

See paragraph 481.

1228. At all times on and from 1 March 2016, Customer 21 should have been recognised by Crown Melbourne as a high risk customer by reason of the matters pleaded at paragraphs 1225, 1229, 1230, 1231, 1232, 1233, 1235 and 1238.

Particulars

Section 36(1)(a), (b) of the Act and Chapter 15 of the Rules.

1229. On and from 1 March 2016, designated services provided to Customer 21 posed higher ML/TF risks including because the provision of designated services to Customer 21 involved a combination of the following factors:

a. Customer 21 was assigned a pseudonym and pseudonym PID which recorded gaming activity and was known only to Crown Melbourne staff members with a certain security level clearance: see paragraph 680(e);

b. designated services provided to Customer 21 lacked transparency as the services were provided under his pseudonym and pseudonym PID: see paragraph 680(e);

c. Customer 21 was a junket player under his pseudonym and pseudonym PID;

d. Customer 21 was a foreign PEP: see paragraphs 118 and 663;

e. Customer 21 received high value financial (table 1, s6) and gaming services (table 3, s6) provided through a junket programs under his pseudonym and pseudonym PID: see paragraph 473ff;

f. between 29 June 2018 and 29 August 2018, Customer 21 had a junket turnover which exceeded $183,000,000 under his pseudonym and pseudonym PID;

g. by 2018, Crown Melbourne recorded Customer 21's individual rated gaming activity to be a cumulative loss of $143,048,106;

h. Customer 21 was known at all times to be connected under his pseudonym and pseudonym PID to the junket operator Customer 2, in respect of whom Crown Melbourne had formed suspicions**;**

i. designated services provided to Customer 21 under his pseudonym and pseudonym PID lacked transparency as the services were provided through the channel of junket programs: see paragraph 477(e);

j. designated services provided to Customer 21 involved large transfers to and from third parties, including from junket operators and to unknown third party companies: see paragraph 456ff;

k. designated services provided to Customer 21 involved large cross-border movements of funds, including through a Southbank account: see paragraph 239;

l. large values were transferred to and from Customer 21's bank accounts and his DAB account, and to and from other customers' DAB accounts, involving the provision by Crown Melbourne of designated services within the meaning of items 31 and 32, table 1, s6 of the Act: see paragraphs 411ff and 492;

m. at various times, Customer 21 had significant parked or dormant funds in his DAB accounts: see paragraph 252;

n. Customer 21 engaged in other transactions indicative of ML/TF typologies and vulnerabilities, including CVIs large account balance, the use of potential shell companies and cuckoo smurfing: see paragraph 24;

o. Crown Melbourne made available the Crown private jet for Customer 21 under his pseudonym and pseudonym PID. There were inadequate controls on the carrying of large amounts of cash on Crown's private jet: see paragraphs 454 and 491(c);

p. these transactions took place against the background of:

   i. between 3 September 2008 and 13 March 2009, on multiple occasions, Customer 21 sent telegraphic transfers to his wife totalling $20,500,000. Crown Melbourne suspected that these transactions, at least in part, were not for gaming purposes;

   ii. by 1 March 2016, Customer 21 had been involved in several large transactions third parties and company accounts. Crown Melbourne suspected that these transactions, at least in part, were not for gaming purposes;

   iii. by 1 March 2016, Customer 21 had been involved in transactions indicative of the ML/TF typology of cuckoo smurfing;

   iv. 28 SMRs being given to the AUSTRAC CEO by Crown Melbourne by 1 March 2016; and

q. by reason of the matters set out at subparagraphs a. to p. above, there were higher ML/TF risks associated with Customer 21's source of wealth/funds.

Monitoring of Customer 21's transactions

1230. Crown Melbourne was unable to monitor the ML/TF risks posed by Customer 21's transactions appropriately because it assigned to him a pseudonym and a pseudonym PID.

Particulars

See paragraph 680(e).

By 8 July 2014, Customer 21 was assigned a pseudonym and pseudonym PID that was linked to his primary PID.

Customer 21 requested that a pseudonym PID be created for privacy reasons and in order to prevent the recording of his gaming activity in connection with his name.

Customer 21 recorded significant gaming activity under his pseudonym and pseudonym PID.

At least some individuals involved in transaction monitoring at Crown Melbourne were unaware of Customer 21's pseudonym and pseudonym PID. On 11 September 2017, Crown Melbourne recorded in an SMR that Customer 21 was not a key player on any recent Customer 2 junket program in connection with a transfer of $2,732,581 from Customer 2 to Customer 21: see particulars to paragraph 1233. However, Customer 21 had played in several Customer 2 junket programs under his pseudonym and pseudonym PID on and from March 2016, including in September 2017.

1231. At no time did Crown Melbourne appropriately monitor Customer 21's transactions on a risk-basis.

Particulars

Section 36(1)(a), (b) of the Act and rules 15.4 to 15.8 of the Rules.

See paragraph 1230.

Crown Melbourne was unable to monitor the ML/TF risks posed by Customer 21's transactions appropriately because it did not make and keep appropriate records of designated services provided to junket players: see paragraphs 483ff.

Crown Melbourne did not apply appropriate risk-based transaction monitoring to designated services provided to Customer 21: see paragraphs 590ff, 629 to 642 and 643 to 649.

Customer 21's transactions involved repeated transactions indicative of ML/TF typologies and vulnerabilities that were not detected prior to a 2021 lookback. Had appropriate risk-based transaction monitoring been applied, these transactions could have been identified earlier: see paragraphs 686 and 687.

Transactions indicative of ML/TF typologies – CVIs large account balance

Transactions involving Customer 21 were identified as indicative of the ML/TF typology of CVIs large account balance by an independent auditor in 2021. Customer 21 had a DAB account balance of $160,000 as at 30 April 2021 which had remained dormant for 473 days.

Transactions indicative of ML/TF typologies – use of potential shell companies and cuckoo smurfing

Transactions involving Customer 21 were identified as indicative of the ML/TF typologies of cuckoo smurfing by an independent auditor in 2020 and use of potential shell companies by an independent auditor in 2021. Company 7 sent transactions totalling $3,999,904 to Customer 21 through a Southbank account. This third party company had also sent telegraphic transfers to the junket operator Customer 15:

- on 7 October 2016, transaction of $1,099,976;

- on 10 October 2016, transaction of $899,976;
- on 14 October 2016, transaction of $1,049,976; and
- on 22 October 2016, transaction of $949,976.

Transactions indicative of ML/TF typologies – parked funds

Transactions involving Customer 21 were identified as indicative of the ML/TF typology of parked funds by an independent auditor in 2021.

From 9 January 2020 to at least 18 June 2021, Customer 21 had a DAB account balance of $1,000,126.

Inadequate controls on Crown's private jets

On 27 May 2016, Crown Melbourne made available the Crown private jet for Customer 21 under his pseudonym and pseudonym PID. The Crown private jet flew from a foreign country to the Gold Coast in order to transport Customer 21, together with six other people, from the Gold Coast to Melbourne.

There were inadequate controls on the carrying of large amounts of cash on Crown's private jets: see paragraphs 454 and 491(c).

Ongoing customer due diligence

1232. On and from 1 March 2016, on multiple occasions, the provision of designated services to Customer 21 raised red flags reflective of higher ML/TF risks as a result of Customer 21's frequent transactions with several foreign third party companies.

Particulars

See paragraph 456ff.

Third party transactions in 2016

On 4 March 2016, Customer 21 sent a telegraphic transfer of $100,000 to a third party company: SMR dated 4 March 2016.

Third party transactions in 2018

On 20 August 2018, Customer 21 sent a telegraphic transfer in a foreign currency to a foreign third party company: SMR dated 21 August 2018.

Third party transactions in 2019

On 16 January 2019, Customer 21 sent a telegraphic transfer in a foreign currency to a foreign third party company: SMR dated 17 January 2019.

1233. On and from 1 March 2016, on multiple occasions, the provision of designated services to Customer 21 raised red flags reflective of higher ML/TF risks as a result of:

a. his junket play, which involved high turnover that was recorded to his pseudonym PID; and

b. complex, unusual large transactions and unusual patterns of transactions involving Customer 21 which had no apparent economic or visible lawful purpose.

Particulars

See paragraphs 420ff and 477.

Unusual transactions and patterns of transactions in 2016

In 2016, Crown Melbourne recorded Customer 21's individual gaming activity to be a loss of $4,910,333.

In 2016, Customer 21 appeared under his pseudonym and pseudonym PID in multiple daily table games program reports and operating reports, including in connection with substantial gaming activity.

Unusual transactions and patterns of transactions in 2017

On 11 September 2017, Customer 21 received a transfer of $2,732,581 from the junket operator, Customer 2. Crown Melbourne noted in an SMR that Customer 21 was not a junket player under any recent Customer 2 junket: SMR dated 13 September 2017. However, Customer 21 was a key player in a September 2017 Customer 2 junket under his pseudonym and pseudonym PID.

Unusual transactions and patterns of transactions in 2018

In 2018, Crown Melbourne recorded Customer 21's individual gaming activity to be a loss of $442,805.

Between 29 June and 29 August 2018, Customer 21 was a key player in Customer 2's junket under his pseudonym and pseudonym PID with an estimated turnover of $183,334,795.

Unusual transactions and patterns of transactions in 2019

Between August 2000 and January 2019, Crown Melbourne recorded Customer 21's cumulative individual gaming activity to be a loss of $145,405,081.

Between 23 March 2018 and 13 February 2019, Customer 21 was investigated by Crown Melbourne 33 times under his pseudonym and pseudonym PID relating to baccarat gaming activity. The total amount of funds investigated or reviewed was $12,516,190. The sums investigated ranged from approximately $250,000 to $720,000. Crown Melbourne also investigated Customer 2 and Customer 21's primary name and PID in relation to some of these amounts.

Customer 21, under his pseudonym and pseudonym PID, was the sole key player on a Customer 2 junket program commencing on 16 December 2019.

1234. At no time did Crown Melbourne undertake appropriate risk-based customer due diligence with respect to Customer 21 or his pseudonym and pseudonym PID with a view to identifying, mitigating and managing the ML/TF risks posed by the provision of designated services on and from 1 March 2016.

a. Crown Melbourne took steps to understand Customer 21's source of wealth/funds. However, Crown Melbourne did not take appropriate steps to determine that Customer 21's source of wealth/funds was legitimate.

b. At no time did Crown Melbourne take appropriate steps to identify or analyse the ML/TF risks of Customer 21's transactions, including transactions under his pseudonym and pseudonym PID, or to consider whether they had a lawful purpose. Crown Melbourne only considered large and high risk third party transactions involving Customer 21 after a substantial period of time had elapsed.

c. At no time did Crown Melbourne give appropriate consideration to whether large and high risk transactions should be processed.

d. At no time did senior management consider whether continuing the business relationship with Customer 21 was within Crown Melbourne's ML/TF risk appetite.

e. Senior management determined that assigning Customer 21 with a pseudonym and pseudonym PID was within Crown Melbourne's ML/TF risk appetite.

Particulars

Section 36(1)(a) of the Act.

The due diligence steps taken with respect to Customer 21 included:

Wealth and risk intelligence reports

In May 2016, September 2016 and November 2020, Crown Melbourne obtained wealth reports in respect of Customer 21. The reports identified Customer 21's business interests and high net worth and source of wealth/funds. The November 2020 wealth report again identified Customer 21's membership of a several foreign political bodies. Despite this, at no point did Crown Melbourne identify Customer 21 to be a foreign PEP.

In December 2020, Crown Melbourne obtained a risk intelligence report in respect of Customer 21. The report identified that Customer 21 was a foreign PEP due to his membership of a several foreign political bodies. Despite this, at no point did Crown Melbourne identify Customer 21 to be a foreign PEP.

None of these searches constituted appropriate steps to understand whether Customer 21's source of wealth/funds was legitimate.

Other due diligence searches

Between May 2016 and November 2020, Crown Melbourne obtained information in respect of companies associated with Customer 21.

Between May 2016 and November 2020, Crown Melbourne conducted land registry, property valuation, Australian bankruptcy, Australian company and foreign company searches in respect to Customer 21.

Between May 2016 and November 2020, Crown Melbourne conducted risk intelligence searches in respect of Customer 21.

In November 2020, Crown Melbourne conducted visa and open source media searches in respect of Customer 21.

None of these searches constituted appropriate steps to understand whether Customer 21's source of wealth/funds was legitimate.

Senior management engagement and transaction monitoring

In August 2019, the Group General Manager (AML) requested further details in respect of Customer 21's March 2016, August 2018 and January 2019 transactions to several foreign third party companies. The CTRM provided SYCO screenshots identifying the three transactions. No further action was taken in respect of these large and suspicious third party transactions.

In August 2019 the Group General Manager (AML) requested further details in respect of the third party company, Company 14, that Customer 21 received telegraphic transfers from 2011 and 2013 totalling $6,581,473.15. Australian company searches identified that Customer 21 was not a director or shareholder of the company. No further action was taken in respect of these large and suspicious third party transactions.

As at 24 August 2021, Customer 21 was the subject to a Significant Player Review.

In late 2020, the Significant Player Review (**SPR**) process was introduced following a recommendation from an independent consultant. It is triggered where a customer spends over $100,000 in the previous 12 months, or $50,000 in a single month. The SPR process ascribes the patron a risk rating which, from lowest to highest risk, may be green, amber, red or black.

Senior management failed to consider at any time whether a business relationship with Customer 21 was within Crown Melbourne's ML/TF risk appetite

None of these steps were proportionate to the ML/TF risks reasonably posed by Customer 21 on and from 1 March 2016.

Enhanced customer due diligence

1235. Having formed a suspicion for the purposes of s41 of the Act, Crown Melbourne gave the AUSTRAC CEO SMRs with respect to Customer 21 on:

a. 4 March 2016;

b. 13 September 2017;

c. 21 August 2018; and

d. 17 January 2019.

Particulars

The SMRs reported Customer 21's annual losses, transfers to other Crown Melbourne patrons and from Crown Melbourne junket

operators, telegraphic transfers to third parties including company accounts and the amount of cash Customer 21 was prepared to carry.

1236. On each occasion that Crown Melbourne formed a suspicion with respect to Customer 21 for the purposes of s41 of the Act, it was required to apply its ECDD program to Customer 21.

Particulars

Rule 15.9(3) of the Rules.

1237. Crown Melbourne did not carry out appropriate risk-based ECDD measures with respect to Customer 21 on each occasion that Crown Melbourne formed a suspicion with respect to Customer 21 for the purposes of s41 of the Act.

a. There are no records of ECDD being conducted following the lodgement of SMRs on 13 September 2017, 21 August 2018 or 17 January 2019: see paragraphs 664 and 685.

b. Other than after giving the AUSTRAC CEO the SMR dated 4 March 2016, appropriate risk-based steps were not taken to obtain or analyse information about Customer 21's source of wealth/funds: see paragraph 667.

c. Other than after giving the AUSTRAC CEO the SMR dated 4 March 2016, appropriate risk-based steps were not taken to analyse and monitor Customer 21's transactions – both past and future – including to understand their economic purpose: see paragraph 590 and 666.

d. At no time did senior management consider whether continuing the business relationship with Customer 21 was within Crown Melbourne's ML/TF risk appetite.

Particulars

Rules 15.9(3), 15.10(1)(c), (d), (2), (5) and (6) of the Rules.

After lodging SMRs on 4 March 2016, Crown Melbourne conducted company, land registry, bankruptcy and risk intelligence searches together with obtaining a wealth report in respect of Customer 21.

See particulars to paragraph 1234.

1238. At all times from 1 March 2016, Customer 21 was a foreign PEP.

Particulars

Section 36(1)(a) of the Act.

By 1 March 2016, Crown Melbourne was aware that Customer 21 was a member of a several foreign political bodies: see particulars to paragraph 1225.

In December 2020, a risk intelligence report obtained by Crown Melbourne further identified Customer 21 to be a foreign PEP: see particulars to paragraph 1234.

However, at no point did Crown Melbourne identify that Customer 21 was a foreign PEP.

1239. At all times from 1 March 2016, Crown Melbourne was required to apply its ECDD program to Customer 21.

Particulars

Rules 15.9(2), 15.11 of the Rules

See paragraphs 660, 663 and 666.

1240. Crown Melbourne did not carry out appropriate risk-based ECDD measures with respect to Customer 21 on and from 1 March 2016 given his status as a foreign PEP. In particular:

a. Crown Melbourne did not undertake a detailed analysis of Customer 21's KYC information or analyse the legitimacy of Customer 21's source of wealth/funds;

b. no steps were taken to seek and obtain senior management approval for continuing a business relationship with Customer 21 having regard to the ML/TF risks posed by the customer; and

c. no steps were taken to seek and obtain senior management approval for whether Crown Melbourne should continue to provide designated services to Customer 21.

Particulars

Rules 15.10(2), 15.10(6), 15.11 of the Rules.

Crown Melbourne conducted various company, land registry, bankruptcy and risk intelligence searches in respect of Customer 21 in May 2016, September 2016, August 2018 and November 2020 together with obtaining wealth and risk intelligence reports. However, these searches were not conducted with a view to identifying, mitigating and managing the ML/TF risk posed by Customer 21 given his status as a foreign PEP.

See particulars to paragraphs 1234 and 1237.

See paragraph 660, 663, 666, 667 and 668.

1241. By reason of the matters pleaded from paragraphs 1222 to 1240, on and from 1 March 2016, Crown Melbourne:

a. did not monitor Customer 21 in relation to the provision of designated services, with a view to identifying, mitigating and managing the ML/TF risks it reasonably faced; and

b. did not do so in accordance with rr 15.5 and 15.9 of the Rules.

1242. By reason of the matters pleaded at paragraph 1241, Crown Melbourne contravened s36(1) of the Act on and from 1 March 2016 with respect to Customer 21.

Particulars

Section 36(1) of the Act is a civil penalty provision: s36(2) of the Act.

Customer 22

1243. Customer 22 has been a customer of Crown Melbourne since at least June 2015 to September 2021.

1244. From 17 March 2017 to September 2021, Crown Melbourne provided Customer 22 with designated services within the meaning of table 1 and table 3, s6 of the Act.

Particulars

On 17 March 2017, Crown Melbourne opened a DAB account and safekeeping account for Customer 22 under two of his PIDs. Customer 22 was a domestic program player: SMR dated 29 November 2021.

Between 2015 and 2018, Customer 22 engaged in at least 385 transactions at Crown Melbourne totalling $18,752,228.

In 2017, Customer 22 had a turnover of $579,377,684 at Crown Melbourne with losses of $1,612,555.

In 2018, Customer 22 had a turnover of $119,146,420 at Crown Melbourne with losses of $3,240,920.

Customer 22 did not have any rated play at Crown Melbourne between 2019 and 2021.

On 16 September 2021, Crown Melbourne issued a WOL in respect of Customer 22.

The ML/TF risks posed by Customer 22

1245. At all times on and from late November 2017, Customer 22 should have been recognised by Crown Melbourne as a high risk customer by reason of the matters pleaded at paragraphs 1247, 1248, 1249, 1250, 1251 and 1253.

Particulars

Section 36(1)(a), (b) of the Act and Chapter 15 of the Rules.

1246. It was not until 26 August 2021 that Customer 22 was rated high risk by Crown Melbourne.

Particulars

On various occasions between 27 March 2017 and 17 January 2018, Crown Melbourne assessed Customer 22 as moderate risk.

On various occasions between 18 January 2018 and 28 November 2019, Crown Melbourne assessed Customer 22 as significant risk.

This was despite Customer 22's frequent large and unusual transactions to third parties.

See paragraph 120.

1247. On and from late November 2017 designated services provided to Customer 22 posed higher ML/TF risks including because the provision of designated services to Customer 22 involved a combination of the following factors:

a. Customer 22 received high value financial (table 1, s6) and gaming services (table 3, s6);

b. Customer 22 was known at all times to be connected to junket operators, including Customer 1 and Customer 2 in respect of whom Crown Melbourne or Crown Perth had formed suspicions. On several occasions, Customer 22 engaged in transactions with representatives from the Suncity or Customer 2 junkets;

c. Customer 22 was known to be connected to Customer 26, who was subsequently issued with a WOL due to his alleged connections to human trafficking;

d. Customer 22 transacted using large amounts of cash and cash that appeared suspicious, including large volumes of cash in carry bags and plastic bags with writing on the side of them: see paragraphs 450, 451 and 452;

e. between 2017 and 2018, Customer 22 made:

   i. 97 incoming cash transactions totalling $5,736,800; and

   ii. 288 outgoing cash transactions totalling $13,015,428;

f. designated services provided to Customer 22 involved large transfers to and from third parties, including to and from other junket operators, foreign remittance service providers and unknown third parties: see paragraph 456ff;

g. between 2017 and 2018, Customer 22 received 335 telegraphic transfers totalling $13,020,110. Of these, 113 telegraphic transfers totalling $1,973,810 were identified as being connected to 36 different third party individuals;

h. on multiple occasions, payments into a Southbank account for Customer 22 were accompanied by payment descriptions that conflicted with the underlying purpose of the payment;

i. designated services provided to Customer 22 involved large cross-border movements of funds, including through a Southbank account and a Riverbank account: see paragraph 239;

j. large values of funds were transferred to and from Customer 22 bank accounts and his DAB account, involving designated services within the meaning of items 31 and 32, table 1, s6 of the Act. Customer 22 used at least 17 Australian bank accounts to complete telegraphic transfers;

k. from November 2017, Customer 22 made a number of cash deposits and withdrawals at the Suncity administration desk, despite not being a player on any Suncity junkets;

l. at various times, Customer 22 had significant parked or dormant funds in his DAB accounts: see paragraph 252;

m. Customer 22 engaged in other transactions indicative of ML/TF typologies and vulnerabilities, including offsetting (including with unrelated third parties), cashing-in large value chips with no evidence of play, and quick turnover of money (without betting): see paragraph 24;

n. as a result of a 2018 lookback, Crown Melbourne concluded that Customer 22's regular deposit and withdrawal of cash and telegraphic transfers could indicate a possible attempt to layer funds and the use of cash, multiple bank accounts, inconsistent narratives and third parties could be an attempt to disguise the source of the funds and make it difficult for Crown to determine the legitimacy of the fund used by Customer 22; and

o. by reason of the matters set out at subparagraphs a. to n. above, there were real risks that Customer 22's source of wealth and source of funds were not legitimate.

Monitoring of Customer 22's transactions

1248. At no time did Crown Melbourne appropriately monitor Customer 22's transactions on a risk-basis.

Particulars

Section 36(1)(a), (b) of the Act and rules 15.4 to 15.8 of the Rules.

Crown Melbourne did not apply appropriate risk-based transaction monitoring to designated services provided to Customer 22: see paragraphs 590ff and 629 to 642.

Customer 22's transactions involved repeated transactions indicative of ML/TF typologies that were not detected prior to a 2021 look-back. Had appropriate risk-based transaction monitoring been applied, these transactions could have been identified earlier: see paragraphs 686 and 687.

Crown Melbourne's 2018 lookback

Customer 22 engaged in the following transactions at Crown Melbourne between 2015 and 2018 (SMR dated 29 November 2021):

- 97 incoming cash transactions totalling $5,736,800;
- 288 outgoing cash transactions totalling $13,015,428;
- 167 sub-threshold transactions via his DAB account comprising 67 incoming cash transactions totalling $217,994 and 102 outgoing cash transactions totalling $285,951;
- in 2017, Customer 22 deposited six bank cheques totalling $1,240,000;
- on 2 June 2017, a total of $150,942 comprising $143,520 in chips, $7,422 in commission and $500 in program points was deposited to Customer 22's DAB account. A total of $151,446 was withdrawn as cash. Following the cash withdrawal, Customer 22 made two telegraphic transfers. In the lookback, Crown Melbourne concluded it was unusual that Customer 22 would continue to send telegraphic transfers to Crown Melbourne when he had taken cash that could be re-used for gaming purposes;
- on 7 June 2017, a total of $63,160 comprising $60,070 in chips and $3,090 commission was deposited to Customer 22's DAB account. Customer 22 then withdrew $63,160 in cash. On the same day, Customer 22 received five telegraphic transfers. In the lookback, Crown Melbourne concluded it was unusual that Customer 22 would continue to send telegraphic transfers to Crown Melbourne when he had taken cash that could be re-used for gaming purposes;
- on 2 January 2018, a total of $213,756 comprising $21,400 in cash, $12,761 in commission, $50,000 in telegraphic transfer and $129,595 in chips was deposited in Customer 22's DAB account.

A total of $213,695 comprising $74,300 in chip purchase vouchers and $139,395 in cash was withdrawn from Customer 22's DAB; and

- following the cash withdrawal, Customer 22 made six telegraphic transfers. In the lookback, Crown Melbourne concluded it was unusual that Customer 22 would continue to send telegraphic transfers to Crown Melbourne when he had taken cash that could be re-used for gaming purposes. Five of these telegraphic transfers were not received into Crown Melbourne's bank account.

Crown Melbourne's 2021 lookback

In addition to the above, between 2017 and 2018 at Crown Melbourne (SMR dated 29 November 2021):

- Customer 22 received 335 telegraphic transfers totalling $13,020,110. Of these, 113 telegraphic transfers totalling $1,973,810 were identified as being connected to 36 different third party individuals;
- Crown Melbourne identified ten incoming telegraphic transfers totalling $2,430,000 originating from cash deposits conducted at an Australian bank;
- Customer 22 sent seven telegraphic transfers totalling $6,216,705. Two of these were sent to third parties, including Person 28;
- between 30 December 2017 and 7 January 2018, Crown Melbourne early released 10 telegraphic transfers totalling $977,000 which were allegedly transferred by Customer 22 to credit Customer 22. This constituted item 6 table 1 services. However, the funds were never credited to Crown Melbourne's bank account;
- Crown Melbourne also identified a number of inconsistent statement narratives used in transactions to or from Customer 22 that did not correspond to gaming; and
- Customer 22 used at least 17 Australian bank accounts to complete telegraphic transfers.

Transactions indicative of ML/TF typologies – Quick Turnover (without betting)

Transactions involving Customer 22 at Crown Melbourne were identified as indicative of the ML/TF typology of quick turnover (without betting) by an independent auditor in 2021.

The following transactions by Customer 22 were identified as involving the deposit of cash or telegraphic transfers and withdrawal of 70% or more of the deposit amount within a 48 hour period:

- On 2 April 2017, Customer 22 deposited $170,000 by cash, then withdrew $1,200,000 from his DAB account by telegraphic transfer on the same day.
- On 6 April 2017, Customer 22 deposited $55,000 by cash, then withdrew $281,738 from his DAB account by telegraphic transfer on the same day.
- On 2 June 2017, Customer 22 deposited $25,000 by telegraphic transfer, then withdrew $151,446 cash from his DAB account over four transactions on the same day.
- On 6 June 2017, Customer 22 deposited $20,000 by telegraphic transfer, then deposited $65,000 by telegraphic transfer over three transactions on 7 June 2017, then withdrew $63,160 cash from his DAB account on the same day.
- On 2 January 2018, Customer 22 deposited $50,000 by telegraphic transfer and $21,400 by cash over two transactions, then withdrew $139,395 cash from his DAB account on the same day.

The audit found that Customer 22 was one of 11 patrons responsible for 66% of the total value of identified quick turnover transactions, despite being only 22% of the total instances.

Transactions indicative of ML/TF typologies – Large holding balances

Transactions involving Customer 22 at Crown Melbourne were identified as indicative of the ML/TF typology of large holding balances by an independent auditor in 2021.

As at 30 April 2021, Customer 22 had a balance of $304,376 in his safekeeping account. At the time of the audit, the balance was unclaimed for 1,162 days since Customer 22's last transaction. Crown Melbourne advised the auditor that the balance was associated with an outstanding debt Customer 22 owed to Crown Melbourne, and that the account could not be closed until the debt was fully serviced.

Transactions indicative of ML/TF typologies – Third party agents

Transactions involving Customer 22 at Crown Melbourne were identified as indicative of the ML/TF typology of use of third party agents by an independent auditor in 2021.

The audit identified 113 transactions in which the transaction narrative referred to a party other than Customer 22. The transactions were dated between 24 March 2017 and 5 December 2017 a total of $1,973,810 was deposited in sums between $900 and $110,000 from third parties.

Further auditor analysis of Customer 22

Deeper analysis by the auditor revealed:

- at the time of the audit, Customer 22's occupation and nationality could not be reliably established based on the information held by Crown Melbourne;
- between 17 March 2017 and 23 February 2018, Customer 22 had 331 bank transactions with total deposits of $12,023,100 and withdrawals of $6,759,505;
- in June 2017, Customer 22 changed his behaviour significantly and stopped withdrawing funds from his Crown accounts through bank transfers. He continued depositing funds until February 2018;
- of the total $59.6 million Customer 22 deposited into his accounts at Crown Melbourne, $12,000,000 (20%) of these transactions were through bank transfers. Another $12,000,000 (20%) was through telegraphic transfers. $5,900,000 (10%) was through cash at the Cage. The remaining 50% was primarily from commission based play chips;
- in April to June 2017 and November 2017 to January 2018, Customer 22 made cash withdrawals totalling over $1,000,000 each month. These cash withdrawals did not align with Customer 22's gaming or deposit data;
- large withdrawals of cash are unusual given the physical and security practicalities involved for an individual carrying such large volumes of cash;
- there was a change in Customer 22's pattern of behaviour in respect of depositing funds from June 2017 onwards. Customer 22 moved away from bank transfers and largely transacted at the Cage with cash and gaming chips;
- 132 bank transactions totalling $2,182,410 during 2017 that were related to third party individuals. Of these, only one was a transfer from Customer 22 to a third party. The remaining 131 transactions were deposits from third parties into Customer 22's account; and
- Customer 22's gaming data displayed unusual patterns of behaviour.

In addition, an independent audit of the Riverbank accounts and Southbank accounts in November 2020 identified the following instances where payments into a Southbank account for Customer 22 were accompanied by payment descriptions that conflicted with the underlying purpose of the payment:

- on 29 December 2017, a payment in the amount of $100,000 with the description 'Personal investment in Company'; and
- on 2 January 2018 and 4 January 2018, two payments in the amount of $100,000 and $70,000 respectively with the description 'Investment in business'.

Ongoing customer due diligence

1249. On and from late November 2017, on multiple occasions, the provision of designated services to Customer 22 by Crown Melbourne raised red flags reflective of higher ML/TF risks as a result of unusual transactions and patterns of transactions involving Customer 22.

Particulars

See paragraphs 450 and 451.

Between 23 March 2017 and 14 January 2018, Customer 22 was recorded in 116 surveillance log entries at Crown Melbourne. 40 of those entries were for unclaimed bets where Customer 22 had left money at a table. The majority of the remaining entries were for reviews of large wins and player profiling, although nothing suspect was noted about his playing style.

By 17 August 2017, Customer 22 had visited Crown Melbourne 130 times that year: SMR dated 17 August 2017.

On 14 November 2017, Customer 22 requested to cash out $500,000 from his deposit account. When questioned about what the cash was to be used for, Customer 22 stated that he would place them in a safe in his room. A few minutes later, he returned and requested a further $66,000 in cash. Crown Melbourne was of the view that he did not have time to return to his room and deposit the cash from his initial withdrawal before returning to make the second withdrawal. Staff suggested the funds could be transferred to his bank account via telegraphic transfer but Customer 22 insisted on taking the funds in cash: SMR dated 14 November 2017.

In around January 2018, Customer 22 presented $300,000 in cash and asked for it to be deposited into his account. The cash was presented in three separate plastic bags with writing on them. Customer 22 was asked where the cash had come from and Crown Melbourne staff noted that it was not in a form that would have been issued by a bank. Customer 22 told staff that he had received the money from the Suncity junket: SMR dated 2 January 2018.

On 1 January 2018, Customer 26 cashed out $687,000, placed the cash in a Crown bag and gave the bag to Customer 22.

In August 2018, Crown Melbourne recorded three transactions for the exchange of gaming chips to cash for Customer 22, totalling $112,060. Customer 22's rated gaming activity did not support this transaction: SMRs dated 15 August 2018, 20 August 2018.

Customer 22's debt to Crown Melbourne

By December 2017, Customer 22 had played on 26 losing programs at Crown Melbourne. By 30 December 2017, he owed a debt of approximately $977,000 to Crown Melbourne. There was $304,376 in Customer 22's DAB account, which Crown Melbourne held as a result of this debt.

Between February 2018 and September 2020, Crown Melbourne made repeated attempts to contact Customer 22 regarding repayment of the debt, including referring Customer 22 to a debt collector.

1250. On and from late November 2017, on multiple occasions, the provision of designated services to Customer 22 by Crown Melbourne raised red flags reflective of higher ML/TF risks as a result of large and frequent transactions with third parties which had no apparent economic or visible lawful purpose.

Particulars

See paragraph 456ff.

On 11 April 2017, Crown Melbourne received a telegraphic transfer in the amount of $20,000 for Customer 22 from a third party: SMR dated 12 April 2017.

On 12 April 2017, Crown Melbourne received two telegraphic transfers totalling $70,000 for Customer 22 from two third parties. One transfer was in the amount $20,000 and the other was in the amount of $50,000: SMR dated 13 April 2017.

On 2 May 2017, Crown Melbourne received a telegraphic transfer for Customer 22 in the amount of $100,000 from a third party: SMR dated 3 May 2017.

Between 20 March 2017 and 11 July 2017, Customer 22 received transfers from at least 10 different accounts and a number of third parties: SMR dated 11 July 2017.

On 29 November 2017, Crown Melbourne sent a telegraphic transfer in the amount of $100,000 for Customer 22 to a third party: SMR dated 30 November 2017.

On 21 December 2017, Crown Melbourne received a telegraphic transfer in the amount of $220,000 from a third party for Customer 22: SMR dated 22 December 2017.

1251. On and from late November 2017, on multiple occasions, the provision of designated services to Customer 22 by Crown Melbourne raised red flags reflective of higher ML/TF risks as a result of unusual transactions and patterns of transactions between Customer 22 and junket representatives associated with both the Suncity and Customer 2 junkets.

Particulars

See paragraph 477.

In early December 2017, Crown Melbourne staff observed a transaction of $116,000 between Customer 22 and a third party at the Suncity cash administration desk. Neither individual was recorded by Crown Melbourne as playing on the Suncity junket at the time: SMR dated 4 December 2017.

On 2 December 2017, Customer 22 cashed in $120,000 at the Suncity administration desk. Customer 22 was not a player on the Suncity junket at the time.

On 3 December 2012, Customer 22 made two separate deposits of $100,000 and $50,000 at the Suncity administration desk. Customer 22 was not a player on the Suncity junket at the time.

On around 29 December 2017, Customer 22 presented $150,000 in cash at the Suncity administration desk and left immediately afterwards: SMR dated 29 December 2017.

On 30 December 2017:

- Customer 22 and a third party, Person 28, attended the Suncity room, produced approximately $100,000 in cash from a Crown-brand carry bag and handed it to a Suncity staff member who counted it. The third party was handed a receipt which both he and Customer 22 signed. They then left the room: SMR dated 2 January 2018;
- shortly afterwards, Customer 22 and the same third party attended the Suncity room and presented approximately $30,000 in a white A4 envelope at the Suncity administration desk. The money was counted and Customer 22 signed a receipt. Both individuals then left the room: SMR dated 2 January 2018;
- shortly afterwards, Customer 22 and the same third party attended the Suncity room and presented approximately $40,000 in a white A4 envelope at the Suncity administration desk. The money was counted and Customer 22 signed a receipt. Both individuals then left the room: SMR dated 2 January 2018;
- shortly afterwards, Customer 22 and the same third party attended the Suncity room and produced approximately $100,000 in cash from a Crown-brand carry bag and handed it to a Suncity staff member who counted it. Customer 22 signed a receipt. Both individuals then left the room: SMR dated 2 January 2018;
- shortly afterwards, Customer 22 attended the Suncity room and presented $50,000 in cash at the Suncity administration desk; and

Neither Customer 22 nor the third party were observed gaming on 30 December 2017: SMR dated 2 January 2018.

On 1 January 2018, over a three hour period, Customer 22 handed over various bundles of cash to the Suncity cash administration desk totalling $495,000, including:

- $100,000 and $80,000 in cash in a Crown carry bag;
- three sums of $60,000, one sum of $85,000 and one sum of $50,000 in cash: SMR dated 2 January 2018.

Around 9 January 2018, Customer 22 requested a Customer 2 junket representative, Person 50, obtain $200,000 worth of gaming chips from the Suncity cash administration desk, in circumstances where Customer 22 had no connection to the Customer 2 or Suncity junkets.

Nor did he have a connection to the junket representative: SMR dated 9 January 2018.

On 14 January 2018, Customer 22 attended the Suncity room as a guest of a junket player, Person 47. Customer 26 was also attending as a guest. When Person 47 finished play, she left the Suncity room and an unknown amount of gaming chips were deposited at the Suncity administration desk. Customer 26 subsequently withdrew $350,000 in cash from the Suncity administration desk, left the Suncity room and handed the bag of cash to Customer 22 in the lift lobby: SMR dated 15 January 2018.

On 13 January 2018, Crown Melbourne received a telegraphic transfer in the amount of $120,000 for Customer 2's junket. The funds were taken by a Customer 2 junket representative, Person 50, in gaming chips. He then sought to exchange those chips to cash, with no observed play. Later that day, Customer 22 presented $120,000 in cash for deposit into his account. During the transaction, Customer 22 mentioned that he owed Customer 2's junket $400,000: SMR dated 15 January 2018.

On around 17 January 2018, Crown Melbourne received a deposit receipt from a Customer 2 junket representative, Person 50, which stated that a cash deposit of $300,000 had occurred at an Australian bank. The junket representative asked whether Crown Melbourne had received the funds and if they could be accessed. The funds were in Crown Melbourne's account however the junket representative was advised that they could not be accessed until the following day. Customer 22 was seen playing with patrons associated with the junket presentative prior to this conversation. Crown Melbourne was of the view that Customer 22 had been receiving funds through Customer 2's junket account, via the Customer 2 junket representative despite the fact that Customer 22 was not a key player under Customer 2's junket: SMR dated 17 January 2018.

Customer 22's last recorded gaming activity was in January 2018.

1252. At no time did Crown Melbourne undertake appropriate risk-based customer due diligence with respect to Customer 22 with a view to identifying, mitigating and managing the ML/TF risks posed by the provision of designated services on and from late November 2017.

a. At no time did Crown Melbourne take appropriate steps to understand Customer 22's source of wealth/funds, including whether Customer 22's source of wealth/funds was legitimate.

b. At no time did Crown Melbourne take appropriate steps to identify or analyse the ML/TF risks of Customer 22's transactions or to consider whether they had a lawful purpose.

c. At no time did Crown Melbourne give appropriate consideration to whether large and high risk transactions should be processed.

d. Prior to the decision to issue Customer 22 with a WOL in September 2021, there is no record of senior management considering whether continuing the business

relationship with Customer 22 was within Crown Melbourne's ML/TF risk appetite in light of the ML/TF risks posed by Customer 22.

Particulars

Section 36(1)(a) of the Act.

Senior management engagement

In October 2020, Customer 22 was referred to the SPR process (see particulars to paragraph 1234). On 17 March 2021, a recommendation was made to refer Customer 22 to the POI Committee. On 10 August 2021, a Customer Risk Analyst noted that Customer 22 had been referred to the POI Committee but a decision had not yet been made.

Between June and August 2021, Crown Melbourne conducted a number of searches in respect of Customer 22.

None of these steps were proportionate to the ML/TF risks reasonably posed by Customer 22 on and from 1 March 2016.

Senior management decision to WOL

On 15 September 2021, the POI Committee considered Customer 22. The Committee noted Customer 22's unverified source of wealth and occupation, the outstanding debt owed to Crown Melbourne, the unusual transactions between Customer 22 and third parties for large cash sums, Customer 22's association with Customer 26 and recommended Customer 22 be banned.

On 16 September 2021, Crown Melbourne issued a WOL in respect of Customer 22.

Enhanced customer due diligence

1253. Having formed a suspicion for the purposes of s41 of the Act, Crown Melbourne gave the AUSTRAC CEO 28 SMRs between 27 March 2017 and 29 November 2021 with respect to Customer 22: Schedule 3.8.

Particulars

The SMRs reported threshold transactions and Customer 22's gaming activity. The suspicions were based on Customer 22's annual losses, the amounts of cash he was prepared to carry, and threshold transactions from third parties. The SMRs also reported some of Customer 22's transactions associated with the Suncity and Customer 2 junkets as set out in paragraph 1251 above.

1254. On each occasion that Crown Melbourne formed a suspicion with respect to Customer 22 for the purposes of s41 of the Act, it was required to apply its ECDD program to Customer 22.

Particulars

Rule 15.9(3) of the Rules.

1255. Crown Melbourne did not carry out appropriate risk-based ECDD measures with respect to Customer 22 on each occasion that Crown Melbourne formed a suspicion with respect to Customer 22 for the purposes of s41 of the Act.

a. There are no records of ECDD being conducted following the lodgement of any SMRs save for the SMR dated 17 January 2018: see paragraphs 664 and 685.

b. With the exception of searches conducted in January 2018, risk-based steps were not taken to obtain or analyse information about Customer 22's source of wealth/funds.

c. Appropriate risk-based steps were not taken to obtain or analyse information about the legitimacy of Customer 22's source of wealth/funds: see paragraph 667.

d. Appropriate risk-based steps were not taken to analyse and monitor Customer 22's transactions – both past and future – including to understand their economic purpose: see paragraph 590 and 666.

e. Prior to the decision to issue Customer 22 with a WOL in September 2021, there is no record of senior management considering whether continuing the business relationship with Customer 22 was within Crown Melbourne's ML/TF risk appetite in light of the ML/TF risks posed by Customer 22. By September 2021, Customer 22 had not played at Crown Melbourne for several years and Crown Melbourne had been unable to contact him in relation to recovery of the debt Customer 22 owed to Crown Melbourne.

Particulars

Rules 15.9(3), 15.10(1)(c), (d), (2), (5) and (6) of the Rules.

After lodging the SMR on 17 January 2018, the following actions were taken:

- on 18 January 2018, Crown Melbourne's Group Credit Manager (VIP International) provided the CTRM with copies of credit searches undertaken in relation to Customer 22;
- between 20 and 22 January 2018, the VIP Customer Relations team and the Marketing Team provided the CTRM with information relating to Customer 22's occupation, businesses and source of wealth;
- Customer 22's source of funds was not known. Crown Melbourne staffs' understanding was that a percentage of commission was paid to his company for services on a purchased or sold project deal by investors; and
- staff also noted that when Customer 22 was winning he tended to cash out and deposit back to his bank account. Customer 22 had told Crown Melbourne that this caused confusion for his bank and the Australian Taxation Office and therefore there was a hold in place on his bank account to hold off on payment of the transfer to Crown Melbourne.

There is no evidence of any further action taken by Crown with respect to Customer 22 following this due diligence.

See particulars to paragraph 1252.

1256. By reason of the matters pleaded from paragraphs 1243 to 1255, on and from 1 March 2016, Crown Melbourne:

a. did not monitor Customer 22 in relation to the provision of designated services, with a view to identifying, mitigating and managing the ML/TF risks it reasonably faced; and

b. did not do so in accordance with rr 15.5 and 15.9 of the Rules.

1257. By reason of the matters pleaded at paragraph 1256, Crown Melbourne contravened s36(1) of the Act on and from 1 March 2016 to 16 September 2021 with respect to Customer 22.

Particulars

Section 36(1) of the Act is a civil penalty provision: s36(2) of the Act.

Customer 23

1258. Customer 23 was a customer of Crown Melbourne between November 2002 and 16 December 2019.

1259. From at least December 2006 to 16 December 2019, Crown Melbourne provided Customer 23 with designated services within the meaning of table 1, s6 table 3, s6 and of the Act.

Particulars

In April 2016, Customer 23 exchanged gaming chips for cash which totalled $34,000.

On 31 July 2017, Crown Melbourne opened a DAB account and safekeeping account (AUD) for Customer 23.

Between 2007 and 2015, Customer 23 had a cumulative loss of $1,458.

Between 2016 and 2018, Customer 23 had a cumulative loss of $4,066.

On 16 December 2019, Crown Melbourne issued a WOL in respect of Customer 23.

1260. From at least 21 September 2017, Customer 23 received designated services as a junket player, facilitated through the Suncity junket.

Particulars

Customer 23 received designated services through the Suncity junket.

The ML/TF risks posed by Customer 23

1261. At all times on and from September 2017, Customer 23 should have been recognised by Crown Melbourne as a high risk customer by reason of the matters pleaded at paragraphs 1263, 1265, 1266 and 1268.

Particulars

Section 36(1)(a), (b) of the Act and Chapter 15 of the Rules.

1262. It was not until 21 December 2018 that Customer 23 was rated high risk by Crown Melbourne.

Particulars

On various occasions between 14 April 2016 and 3 April 2018, Crown Melbourne assessed Customer 23 as moderate risk.

On various occasions between 21 September 2017 and 4 December 2018, Crown Melbourne assessed Customer 23 as significant risk.

On various occasions between 21 December 2018 and 3 July 2020, Crown Melbourne assessed Customer 23 as high risk.

This was despite Customer 23's significant junket activity and that, in September 2017, Customer 23 reported that a large amount of cash was reported stolen from his car and Customer 23 was the subject of a law enforcement inquiry.

See paragraph 481.

1263. On and from September 2017 designated services provided to Customer 23 posed higher ML/TF risks including because the provision of designated services to Customer 23 involved a combination of the following factors:

a. Customer 23 was a junket player with the Suncity junket;

b. Customer 23 received high value financial (table 1, s6) and gaming services (table 3, s6) provided through a junket program: see paragraph 473ff;

c. designated services provided to Customer 23 including large telegraphic transfers to junket operators;

d. Customer 23 was known at all times to be connected to the Suncity junket operator in respect of whom Crown Melbourne had formed suspicions;

e. Customer 23 transacted using large amounts of cash and cash that appeared suspicious, including large volumes of cash in small notes contained in brown cardboard bags: see paragraphs 450, 451 and 452;

f. by 15 January 2019, Crown Melbourne was aware that Customer 23, while on Crown Melbourne premises, had received a backpack containing $250,000 in cash from a Suncity employee and attempted to deposit the cash into a flagged bank account;

g. between 26 September 2017 and 13 December 2019, Customer 23 was the subject of multiple law enforcement inquiries;

h. by December 2019, Crown Melbourne was aware that Customer 23 would be charged with dealing with the proceeds of crime and dealing with property suspected to be the proceeds of crime;

i. by 21 December 2018, Crown Melbourne was aware that the two forms of identification it had for Customer 23 contained images of different persons; and

j. by reason of the matters set out at subparagraphs a. to i. above, there were real risks that Customer 23's source of wealth and source of funds were not legitimate.

Monitoring of Customer 23's transactions

1264. At no time did Crown Melbourne appropriately monitor Customer 23's transactions on a risk-basis.

Particulars

Section 36(1)(a), (b) of the Act and rules 15.4 to 15.8 of the Rules.

Crown Melbourne was unable to monitor the ML/TF risks posed by Customer 23's transactions appropriately because it did not make and keep appropriate records of designated services provided to junket players: see paragraphs 483ff.

Crown Melbourne did not apply appropriate risk-based transaction monitoring to designated services provided to Customer 23: see paragraphs 590ff, 629 to 642 and 643 to 649.

Crown Melbourne did not apply appropriate risk-based transaction monitoring in respect of large and repeated cash deposits made by Customer 23 at the Suncity cash administration desk: see paragraphs 529 to 531.

Ongoing customer due diligence

1265. On and from April 2016, on multiple occasions, the provision of designated services to Customer 23 raised red flags reflective of higher ML/TF risks as a result of complex, unusual large transactions and unusual patterns of transactions involving Customer 23, including numerous cash deposits at the Suncity cash administration desk which had no apparent economic or visible lawful purpose.

Particulars

See paragraphs 477, 450 and 451.

Large and suspicious transactions and patterns of transactions in 2016

In April 2016, Customer 23 was involved in three threshold transactions, being gaming chip to cash exchanges, which totalled $34,000. Customer 23's rated gaming activity did not support the transaction.

Large and suspicious transactions and patterns of transactions in 2017

On 31 July 2017, Customer 23 was a key player in the Suncity junket program. Customer 23 received a telegraphic transfer of $170,000 from Company 1, a money changer. The funds were then transferred to the Suncity junket account.

On 21 September 2017, Customer 23 reported that $210,000 in cash to have been stolen from his car: SMR dated 21 September 2017.

Large and suspicious transactions and patters of transactions in 2018

On 4 December 2018, Customer 23 was a key player on a Suncity junket program. Customer 23 was noted as winning $400,000 during that junket program.

Large and unusual cash deposits at the Suncity cash administration desk

Between 20 October 2017 and 30 March 2018, usually while a key player on the Suncity junket program, Customer 23 deposited approximately $760,000 in cash at the Suncity cash administration desk comprising:

- on 20 October 2017, a person unknown at the time to Crown Melbourne, but later identified to be Customer 23, made a cash deposit at the Suncity cash administration desk of $180,000. The cash was contained in a black bag and a brown cardboard bag. Customer 23 then immediately left the premises;
- on 12 January 2018, Customer 23 deposited approximately $100,000 in cash at the Suncity cash administration desk and then immediately left the premises;
- on 25 January 2018, Customer 23 deposited approximately $130,000 in cash at the Suncity cash administration desk. Customer 23 had won $52,000 with a turnover of $146,750, deposited the chips at the Suncity cash administration desk but did not exchange the chips for cash;
- on 31 January 2018, Customer 23 deposited approximately $150,000 in cash at the Suncity cash administration desk in exchange for chips;
- on 13 March 2018, Customer 23 deposited $100,000 in cash at the Suncity cash administration desk. A Senior Surveillance Operator identified that leaving money in Customer 23's account was something that Customer 23 did regularly; and
- on 30 March 2018, Customer 23 deposited approximately $100,000 in cash at the Suncity cash administration desk. Customer 23 did not have any gaming activity that day to support the deposit.

The 2018 Suncity backpack incident

On 21 December 2018, Crown Melbourne received a law enforcement inquiry in respect of Customer 23. The law enforcement inquiry indicated that on 19 December 2018, Customer 23, together with another Crown Melbourne patron, had attended the parking area of Crown Melbourne in a vehicle where they were met by a person wearing a Suncity tie and handed a backpack containing cash comprising bundles of $50 notes. On 20 December 2018, Customer 23 and the other patron had been taken into custody after attempting to deposit $250,000, being the cash contained in the backpack, into a

flagged Australian bank account. Crown Melbourne conducted a review of the footage available in respect of the Suncity backpack incident, which revealed that the backpack was retrieved from behind the curtains in the Suncity room: SMR dated 21 December 2018.

On 15 January 2019, Crown Melbourne identified the person, being a Suncity employee, that it believed handed the backpack to Customer 23 and the other Crown Melbourne patron: SMR dated 15 January 2019.

1266. On and from April 2016, on multiple occasions, the provision of designated services to Customer 23 raised red flags reflective of higher ML/TF risks as a result of law enforcement inquiries received in respect of Customer 23.

Particulars

On 26 September 2017, 22 October 2018 and 15 July 2019, Crown Melbourne received a law enforcement inquiry in respect of Customer 23.

On 13 December 2019, Crown Melbourne was informed that Customer 23, together with the other Crown Melbourne patron, would be charged with dealing with the proceeds of crime and dealing with property suspected to be the proceeds of crime.

On 13 December 2019, nearly a year after the Suncity backpack incident, the Crown Melbourne POI Committee determined to issue a WOL in respect of Customer 23.

On 16 December 2019, Crown Melbourne issued a WOL in respect of Customer 23.

On 18 June 2020, Customer 23 appeared in the Melbourne Magistrates Court.

1267. It was not until December 2019 that Crown Melbourne undertook appropriate risk-based customer due diligence with respect to Customer 23 with a view to identifying, mitigating and managing the ML/TF risks posed by the provision of designated services on and from 1 March 2016.

a. At no time did Crown Melbourne take appropriate steps to understand whether Customer 23's source of wealth/funds was legitimate.

b. At no time did Crown Melbourne take appropriate steps to identify or analyse the ML/TF risks of Customer 23's transactions or to consider whether they had a lawful purpose, in particular the Suncity cash deposits.

c. At no time did Crown Melbourne give appropriate consideration to whether large and high risk transactions should be processed.

d. Prior to the decision to issue Customer 23 with a WOL in December 2019, there is no record of senior management considering whether continuing the business relationship with Customer 23 was within Crown Melbourne's ML/TF risk appetite in light of the ML/TF risks posed by Customer 23.

Particulars

Section 36(1)(a) of the Act.

The due diligence steps taken with respect to Customer 23 included:

In February 2017 and September 2018, Crown Melbourne conducted a risk intelligence search in respect of Customer 23.

As a result of the law enforcement inquiry on 21 December 2018, an Investigation Manager conducted a review of Customer 23's Crown Melbourne profile. The review included Customer 23's SYCO activity together with Customer 23's foreign driver's licence and passport, which appeared to include images of different persons.

As a result of the law enforcement inquiry on 13 December 2019, a Manager (Compliance Reporting) compiled Customer 23's name, date of birth, Crown rewards number and SYCO activity and recommended that a WOL be issued in respect of Customer 23.

On 16 December 2019, the AML Manager considered Customer 23's gaming history and determined that there had been minimal or no gaming activity since the 21 December 2018 SMR had been given to the AUSTRAC CEO.

On 15 April 2021, Crown Melbourne conducted a company search in respect of Customer 23.

None of these steps were proportionate to the ML/TF risks reasonably posed by Customer 23 on and from 1 March 2016.

Enhanced customer due diligence

1268. Having formed a suspicion for the purposes of s41 of the Act, Crown Melbourne gave the AUSTRAC CEO SMRs with respect to Customer 23 on:

a. 14 April 2016;

b. 21 September 2017;

c. 23 October 2017;

d. 15 January 2018;

e. 29 January 2018;

f. 3 April 2018;

g. 4 December 2018;

h. 21 December 2018; and

i. 15 January 2019.

Particulars

The SMRs reported suspicious activity reflective of a higher ML/TF risk including patterns of transactions unsupported by gaming activity, the amount of cash that Customer 23 was prepared to carry and to leave in his vehicle, large cash transactions, funds presented at the

Suncity cash administration desk with no associated cash withdrawal, significant junket wins and the information relating to the Suncity backpack incident pleaded at paragraph 1265.

1269. On each occasion that Crown Melbourne formed a suspicion with respect to Customer 23 for the purposes of s41 of the Act, it was required to apply its ECDD program to Customer 23.

Particulars

Rule 15.9(3) of the Rules.

1270. Crown Melbourne did not carry out appropriate risk-based ECDD measures with respect to Customer 23 on each occasion that Crown Melbourne formed a suspicion with respect to Customer 23 for the purposes of s41 of the Act.

a. There are no records of ECDD being conducted following the lodgement of SMRs on 14 April 2016, 21 September 2017, 23 October 2017, 15 January 2018, 29 January 2018, 3 April 2018 or 4 December 2018: see paragraphs 664 and 685.

b. Appropriate risk-based steps were not taken to obtain or analyse information about Customer 23's source of wealth/funds: see paragraph 667.

c. Appropriate risk-based steps were not taken to analyse and monitor Customer 23's transactions – both past and future – including to understand their economic purpose: see paragraph 590 and 666.

d. Prior to the decision to issue Customer 23 with a WOL in December 2019, there is no record of senior management considering whether continuing the business relationship with Customer 23 was within Crown Melbourne's ML/TF risk appetite in light of the ML/TF risks posed by Customer 23.

e. Crown Melbourne issued a WOL in respect of Customer 23 a year after the Suncity backpack incident.

Particulars

Rules 15.9(3), 15.10(1)(c), (d), (2), (5) and (6) of the Rules.

The ECDD conducted in connection with the lodgement of the SMRs on 21 December 2018 and 15 January 2019 related primarily to the Suncity backpack incident and only included searches of Crown Melbourne's internal information sources.

On 16 December 2019, Crown Melbourne issued Customer 23 with a WOL. This was nearly six months after Crown Melbourne last provided a designated service to Customer 23.

See particulars to paragraph 1267.

1271. On and from 21 December 2018, Crown Melbourne rated Customer 23 high risk.

Particulars

Crown Melbourne rated Customer 23 high risk on six occasions between 21 December 2018 and 3 July 2020: paragraph 1262.

1272. On each occasion that Crown Melbourne rated Customer 23 high risk, Crown Melbourne was required to apply its ECDD program to Customer 23.

Particulars

Rule 15.9(1) of the Rules.

See paragraph 661.

1273. Crown Melbourne did not carry out appropriate risk-based ECDD measures with respect to Customer 23 on each occasion that Crown Melbourne rated Customer 23 high risk.

Particulars

See particulars to paragraphs 1267 and 1270.

See paragraphs 661, 666, 667 and 668.

1274. By reason of the matters pleaded from paragraphs 1258 to 1273, on and from September 2017, Crown Melbourne:

a. did not monitor Customer 23 in relation to the provision of designated services, with a view to identifying, mitigating and managing the ML/TF risks it reasonably faced; and

b. did not do so in accordance with rr 15.5 and 15.9 of the Rules.

1275. By reason of the matters pleaded at paragraph 1274, Crown Melbourne contravened s36(1) of the Act on and from September 2017 to 16 December 2019 with respect to Customer 23.

Particulars

Section 36(1) of the Act is a civil penalty provision: s36(2) of the Act.

Customer 24

1276. Customer 24 was a customer of Crown Melbourne from 21 December 2014 to December 2019.

1277. From at least 21 December 2014 to December 2019, Crown Melbourne provided Customer 24 with designated services within the meaning of table 1 and table 3, s6 of the Act.

1278. From at least 24 December 2014 to December 2019, Customer 24 received designated services as a junket player, facilitated through three different junket operators, and as a junket representative of a junket.

Particulars to paragraphs 1277 and 1278

Customer 24 received designated services through the Suncity junket and Customer 4's and Person 22's junkets.

On 23 September 2015, Crown Melbourne opened a DAB account and safekeeping account for Customer 24.

Between August 2017 and December 2017, Crown Melbourne recorded Customer 24's junket cumulative turnover to be $11,668,730 and HKD71,338,500 with cumulative losses was $247,890 and HKD370,000.

On 18 December 2019, Crown Melbourne issued a WOL in respect of Customer 24.

The ML/TF risks posed by Customer 24

1279. At all times on and from May 2017, Customer 24 should have been recognised by Crown Melbourne as a high risk customer by reason of the matters pleaded at paragraphs 1281, 1283, 1284 and 1286.

Particulars

Section 36(1)(a), (b) of the Act and Chapter 15 of the Rules.

1280. It was not until 3 May 2018 that Customer 24 was rated high risk by Crown Melbourne.

Particulars

On various occasions between 24 December 2014 and 1 February 2018, Crown Melbourne assessed Customer 24 as moderate risk.

This was despite that, in May 2017, a VCGLR inspector identified that Customer 24 engaged in potential money laundering in the Suncity room. He was handing out money from a cooler bag full of cash in $50 and $100 notes bundled in various sizes.

See paragraph 481.

1281. From May 2017 designated services provided to Customer 24 posed higher ML/TF risks including because the provision of designated services to Customer 24 involved a combination of the following factors:

a. Customer 24 was a junket player;

b. Customer 24 received high value financial (table 1, s6) and gaming services (table 3, s6) provided through the Suncity junket programs: see paragraph 473ff;

c. Customer 24 was known at all times to be connected to junket operators, including junket operators in respect of whom Crown Melbourne or Crown Perth had formed suspicions including Customer 4 and Customer 1;

d. between August 2017 and December 2017, Crown Melbourne recorded Customer 24's junket cumulative turnover to be $11,668,730 and HKD71,338,500 with cumulative losses of $247,890 and HKD370,000;

e. designated services provided to Customer 24 lacked transparency as the services were provided through the channel of junket programs: see paragraph 477(e);

f. Customer 24 transacted using large amounts of cash and cash that appeared suspicious, including one incident where he distributed cash from a blue cooler bag: see paragraphs 450, 451, 452 and 491;

g. Customer 24 was arrested in the Suncity room in May 2018 in connection to a money laundering investigation;

h. Customer 24 presented cheques from other Australian casinos; and

i. by reason of the matters set out at subparagraphs a. to h. above, there were real risks that Customer 24's source of wealth and source of funds were not legitimate.

Monitoring of Customer 24's transactions

1282. At no time did Crown Melbourne appropriately monitor Customer 24's transactions on a risk-basis.

Particulars

Section 36(1)(a), (b) of the Act and rules 15.4 to 15.8 of the Rules.

Crown Melbourne was unable to monitor the ML/TF risks posed by Customer 24's transactions appropriately because it did not make and keep appropriate records of designated services provided to junket players: see paragraphs 483ff.

Crown Melbourne did not apply appropriate risk-based transaction monitoring to designated services provided to Customer 24: see paragraphs 590ff, 629 to 642 and 643 to 649.

Ongoing customer due diligence

1283. From May 2017, the provision of designated services to Customer 24 by Crown Melbourne raised red flags reflective of higher ML/TF risks by reason of an incident involving a cooler bag of cash in the Suncity room and Customer 24's subsequent arrest on money laundering-related charges (unrelated to the cooler bag incident).

Particulars

See paragraphs 450, 451 and 491.

On around 10 May 2017, a VCGLR inspector identified Customer 24 engaging in potential money laundering in the Suncity room. He was handing out money from a cooler bag full of cash (the **cooler bag incident**). The cash was in $50 and $100 notes bundled in various sizes. The VCGLR inspector observed this incident on CCTV footage.

From June 2017 to May 2018, the VCGLR conducted ongoing surveillance of Customer 24 at Crown Melbourne. At the same time, Customer 24 was under criminal investigation by a law enforcement agency for other fraud-related matters unrelated to the cooler bag incident.

Crown Melbourne did not identify Customer 24 as the individual involved in the cooler bag incident until December 2019, approximately two years after the transaction took place. At that time, Crown Melbourne made the decision not to take any further steps to satisfy itself as to the source of funds of the transaction because the transaction was not between Customer 24 and Crown Melbourne.

On 2 May 2018, Customer 24 was arrested by a law enforcement agency in Pit 86. Crown Melbourne was advised that the arrest was a result of an ongoing investigation around deception and money laundering and that they had been trying to catch Customer 24 for a long time. The law enforcement agency further advised that none of the suspected offences had taken place at Crown Melbourne. The arrest did not relate to the cooler bag incident.

On 2 May 2018, Customer 24 was charged with obtaining property by deception for a fraud-related matter and with offences relating to dealing with proceeds of crime.

Customer 24 had no rated play at Crown Melbourne following his arrest.

On 16 December 2019, Crown Melbourne became aware that Customer 24 had been charged with 'fraud related offences'.

On 18 December 2019, Crown Melbourne issued a WOL in respect of Customer 24 and applied stop codes to his account.

1284. From 2017, on multiple occasions, the provision of designated services to Customer 24 by Crown Melbourne raised red flags reflective of higher ML/TF risks by reason of Customer 24's activities on a number of Suncity junket programs.

Particulars

See paragraphs 420ff and 477.

Large and suspicious transactions and patterns of transactions

During the following times, designated services provided to Customer 24 involved complex, unusual large transactions and unusual patterns of transactions which had no apparent economic or visible lawful purpose:

- on 9 January 2017, Customer 24 deposited $70,000 by cheque, then transferred $70,000 from his DAB account to another Crown Melbourne DAB account on the same day;
- on 6 February 2017, Customer 24 deposited $174,000 and $56,000 by cheque, then transferred $230,000 from his DAB account to another Crown Melbourne DAB account on the same day;
- on 14 December 2017, Customer 24 presented a $150,000 cheque from another Australian casino;
- on 15 December 2017, Customer 24 presented $40,000 in cash at the Suncity administration desk for deposit into his account. He did not obtain any chips for gaming. Approximately one hour later, he withdrew $50,000 in cash from the Suncity administration desk: SMR dated 15 December 2017; and
- in January 2018, Crown Melbourne reported a loss of $104,140 for Customer 24 on a Suncity junket: SMR dated 1 February 2018.

Junket play between August 2017 and December 2017

Customer 24 played predominately on junket programs at Crown Melbourne. As a result, his play was not always rated and recorded by Crown Melbourne: see paragraphs 483, 485 and 532

Between August 2017 and December 2017, Crown Melbourne Customer 24 played on ten junket programs with Suncity. His total

turnover on these programs was $11,668,730 and HKD71,338,500. His total loss was $247,890 and HKD370,000:

- between 1 August 2017 and 31 August 2017, Crown Melbourne recorded Customer 24's turnover to be $2,200,000 with a win of $77,170;
- between 1 August 2017 and 30 August 2017 Crown Melbourne recorded Customer 24's turnover to be HKD48,170,000 with a win of HKD797,550;
- between 1 September 2017 and 30 September 2017. Crown Melbourne recorded Customer 24's turnover to be $2,560,000 with a win of $48,830;
- between 1 September 2017 and 30 September 2017, Crown Melbourne recorded Customer 24's turnover to be HKD16,770,000 with a win of HKD659,200;
- between 1 October 2017 and 30 October 2017, Crown Melbourne recorded Customer 24's turnover to be $4,580,000 with a loss of $178,370;
- between 1 October 2017 and 30 October 2017, Crown Melbourne recorded Customer 24's turnover to be HKD6,230,000 with a loss of HKD300,000;
- between 1 November 2017 and 30 November 2017, Crown Melbourne recorded Customer 24's turnover to be $1,300,000 with a loss of $60,890;
- between 1 November 2017 and 30 November 2017, Crown Melbourne recorded Customer 24's turnover to be HKD168,500 with a loss of HKD70,000;
- between 1 December 2017 and 31 December 2017, Crown Melbourne recorded Customer 24's turnover to be $948,730 with a loss of $8,630; and
- on 15 December 2017, a transfer of $150,000 from Customer 24's DAB account to Customer 1's DAB account was voided. It is not clear why this transaction was voided.

Customer 24 played on a Suncity junket in January 2018. There are no records of his play.

Customer 24 played on a Suncity junket in May 2018. There are no records of his play.

1285. At no time did Crown Melbourne undertake appropriate risk-based customer due diligence with respect to Customer 24 with a view to identifying, mitigating and managing the ML/TF risks posed by the provision of designated services from 2017.

a. There are no records showing that Crown Melbourne carried out any due diligence following the cooler bag incident.

b. There are no records showing that Crown Melbourne carried out any due diligence following Customer 24's arrest.

c. There are no record of senior management engagement with Customer 24 until May 2018 at which point the Group General Manager (AML) reviewed due diligence searches that had been conducted in respect of Customer 24 in 2016 and one due diligence search that had been conducted in February 2018.

d. At no time did Crown Melbourne take appropriate steps to understand Customer 24's source of wealth/funds was legitimate.

e. At no time did Crown Melbourne take appropriate steps to identify or analyse the ML/TF risks of Customer 24's transactions or to consider whether they had a lawful purpose.

f. At no time did Crown Melbourne give appropriate consideration to whether large and high risk transactions should be processed.

g. Prior to the decision to issue Customer 24 with a WOL in December 2019, there is no record of senior management considering whether continuing the business relationship with Customer 24 was within Crown Melbourne's ML/TF risk appetite in light of the ML/TF risks posed by Customer 24.

Particulars

Section 36(1)(a) of the Act.

The due diligence steps taken with respect to Customer 24 included:

On 16 May 2018, the Group General Manager (AML) sent Customer 24's due diligence file to the Chief Legal Officer (Australian Resorts). The due diligence file reflects that Crown Melbourne had carried out the following due diligence with respect to Customer 24:

- a risk intelligence search on 5 February 2018;
- open source searches on 12 December 2016; and
- obtained two wealth reports on 12 December 2016.

None of these steps were proportionate to the ML/TF risks reasonably posed by Customer 24 from 2017.

On 18 December 2019, Customer 24 was referred to the POI Committee as an urgent out of meeting request. Customer 24 was subsequently issued with a WOL.

Enhanced customer due diligence

1286. Having formed a suspicion for the purposes of s41 of the Act, Crown Melbourne gave the AUSTRAC CEO SMRs with respect to Customer 24 on:

a. 15 December 2017;

b. 1 February 2018; and

c. 15 December 2021.

Particulars

The SMRs dated 15 December 2017 and 1 February 2018 reported conduct related to Customer 24's activity in connection with Suncity junkets.

The 15 December 2021 SMR reported a transfer from Customer 24 to a third party.

1287. On each occasion that Crown Melbourne formed a suspicion with respect to Customer 24 for the purposes of s41 of the Act, it was required to apply its ECDD program to Customer 24.

Particulars

Rule 15.9(3) of the Rules.

1288. Crown Melbourne did not carry out appropriate risk-based ECDD measures with respect to Customer 24 on each occasion that Crown Melbourne formed a suspicion with respect to Customer 24 for the purposes of s41 of the Act.

a. There are no records of ECDD being conducted following the lodgement of any of the three SMRs submitted in respect of Customer 24: see paragraphs 664 and 685.

b. Appropriate risk-based steps were not taken to obtain or analyse information about Customer 24's source of wealth/funds or to understand the legitimacy of his source of wealth/funds: see paragraph 667.

c. Appropriate risk-based steps were not taken to analyse and monitor Customer 24's transactions – both past and future – including to understand their economic purpose: see paragraph 590 and 666.

d. Prior to the decision to issue Customer 24 with a WOL in December 2019, there is no record of senior management considering whether continuing the business relationship with Customer 24 was within Crown Melbourne's ML/TF risk appetite in light of the ML/TF risks posed by Customer 24.

e. Crown Melbourne issued Customer 24 with a WOL some 18 months after Customer 24 was arrested on Crown Melbourne's premises as a result of an ongoing investigation in respect of deception and money laundering.

Particulars

Rules 15.9(3), 15.10(1)(c), (d), (2), (5) and (6) of the Rules.

See particulars to paragraph 1285.

1289. On and from 3 May 2018, Crown Melbourne rated Customer 24 high risk.

Particulars

Between 3 May 2018 and 22 July 2020, Crown Melbourne rated Customer 24 as high risk on four occasions: see particulars to paragraph 1280.

1290. On each occasion that Crown Melbourne rated Customer 24 high risk, Crown Melbourne was required to apply its ECDD program to Customer 24.

Particulars

Rule 15.9(1) of the Rules.

See paragraph 661.

1291. Crown Melbourne did not carry out appropriate risk-based ECDD measures with respect to Customer 24 after rating Customer 24 high risk on 3 May 2018.

Particulars

See particulars to paragraphs 1285 and paragraph 1288.

See paragraphs 661, 666, 667 and 668.

1292. By reason of the matters pleaded from paragraphs 1276 to 1291, on and from 1 March 2016, Crown Melbourne:

a. did not monitor Customer 24 in relation to the provision of designated services, with a view to identifying, mitigating and managing the ML/TF risks it reasonably faced; and

b. did not do so in accordance with rr 15.5 and 15.9 of the Rules.

1293. By reason of the matters pleaded at paragraph 1292, Crown Melbourne contravened s36(1) of the Act on and from 1 March 2016 to December 2019 with respect to Customer 24.

Particulars

Section 36(1) of the Act is a civil penalty provision: s36(2) of the Act.

Customer 25

1294. Customer 25 has been a customer of Crown Melbourne since 22 November 2014.

1295. From at least 22 November 2014, Crown Melbourne provided Customer 25 with designated services within the meaning of table 1 and table 3, s6 of the Act.

1296. From at least 1 February 2016, Customer 25 received designated services as a junket player, facilitated through four different junket operators.

Particulars to paragraphs 1295 and 1296

Customer 25 attended Crown Melbourne as a junket player under the Suncity, Meg-Star and two other junket programs. Between 1 March 2016 and 4 February 2019, Customer 25 attended at least 19 junket programs at Crown Melbourne.

On 22 November 2014, Crown Melbourne opened a DAB account and safekeeping account (AUD) for Customer 25 which remain open.

Between 2014 and 2018, Crown Melbourne recorded Customer 25's individual rated gaming activity to be a cumulative buy-in of $3,237,625 with a cumulative loss of $677,385.

In FY2015, Crown Melbourne recorded Customer 25's individual gaming activity and gaming activity on junket programs to be a cumulative turnover of $4,333,200 with a loss of $429,060.

In FY2016, Crown Melbourne recorded Customer 25's individual gaming activity and gaming activity on junket programs to be a cumulative turnover of $11,780,650 with a loss of $121,905.

Between 1 October 2017 and 1 November 2018, Crown Melbourne recorded Customer 25's junket activity to be a cumulative turnover of $283,728,860 and HKD24,420,000 with a cumulative loss of $8,778,170 and HKD2,342,100.

Between 1 January 2019 and 4 February 2019, Crown Melbourne recorded Customer 25's junket activity to be a cumulative loss of $500,000: SMR dated 4 February 2019.

The ML/TF risks posed by Customer 25

1297. By 1 March 2016, higher ML/TF risks were indicated by the nature and purpose of Customer 25's business relationship with Crown Melbourne, the nature of the transactions he had been conducting, together with the suspicions Crown Melbourne itself had formed with respect to Customer 25.

Particulars

Section 36(1)(a), (b) of the Act and Chapter 15 of the Rules.

Customer 25 was a junket player. He received designated services through the channel of junket programs. This channel lacked transparency: see paragraph 477.

By 1 March 2016, Crown Melbourne had given the AUSTRAC CEO four SMRs in relation to Customer 25 – on 24 November 2014, 21 October 2015, 1 February 2016 and 1 March 2016. Each SMR reported the same repeated patterns of suspicions relating to high annual individual and junket losses and the amount of cash Customer 25 was prepared to carry.

Collectively, the SMRs given to the AUSTRAC CEO between 24 November 2014 and 1 March 2016 reported total junket losses of $3,232,375.

Between 2014 and 2015, Crown Melbourne recorded Customer 25's individual rated gaming activity to be cumulative buy-in of $1,006,925 and cumulative loss of $573,490.

In FY2015, Crown Melbourne recorded Customer 25's individual gaming activity and gaming activity on junket programs to be a cumulative turnover of $4,333,200 with a loss of $429,060.

By 1 March 2016, Customer 25 had attended at least two junket programs at Crown Melbourne.

By 1 March 2016, no due diligence steps had been taken with respect to Customer 25.

1298. By 1 March 2016, Customer 25 should have been recognised by Crown Melbourne as a high risk customer for the reasons pleaded at paragraph 1297.

Particulars

Section 36(1)(a), (b) of the Act and Chapter 15 of the Rules.

1299. At no time was Customer 25 rated high risk by Crown Melbourne.

Particulars

On various occasions between 24 November 2014 and 26 February 2019, Crown Melbourne assessed Customer 25 as moderate risk.

See paragraph 481.

1300. At all times on and from 1 March 2016, Customer 25 should have been recognised by Crown Melbourne as a high risk customer by reason of the matters pleaded at paragraphs 1297, 1301, 1303, 1304, 1305 and 1307.

Particulars

Section 36(1)(a), (b) of the Act and Chapter 15 of the Rules.

1301. On and from 1 March 2016 designated services provided to Customer 25 posed higher ML/TF risks including because the provision of designated services to Customer 25 involved a combination of the following factors:

a. Customer 25 received high value financial (table 1, s6) and gaming services (table 3, s6) provided through multiple junket programs including Suncity and Meg-Star junkets: see paragraph 473ff;

b. Customer 25 was a junket player;

c. by no later than February 2019, Customer 25's junket turnover had exceeded $301,400,210 and HKD24,420,000;

d. Customer 25 was known at all times to be connected to junket operators, including Customer 1 in respect of whom Crown Melbourne had formed suspicions;

e. designated services provided to Customer 25 lacked transparency as the services were provided through the channel of junket programs: see paragraph 477(e);

f. Customer 25, and persons associated with him, transacted using large amounts of cash and cash that appeared suspicious, including large volumes of cash in small notes bundled inside of backpacks and shopping bags and counterfeit cash: see paragraphs 450, 451, 452 and 491;

g. on multiple occasions, Customer 25 presented to the Suncity cash administration desk with large and suspicious cash despite showing significant losses under Suncity junket programs at the time;

h. designated services provided to Customer 25 involved large transfers to and from third parties, including to and from Customer 1 and unknown third parties: see paragraph 456ff;

i. large values were transferred to and from Customer 25's bank accounts and his DAB account, and to and from other customers' DAB accounts, involving the provision by Crown Melbourne of designated services within the meaning of items 31 and 32, table 1, s6 of the Act: see paragraphs 411ff and 492;

j. Customer 25 and persons acting on Customer 25's behalf engaged in other transactions indicative of ML/TF typologies and vulnerabilities, including refining: see paragraph 24;

k. these transactions took place against the background of four SMRs being given to the AUSTRAC CEO by Crown Melbourne by 1 March 2016;

l. by January 2019, Crown Melbourne were aware of media reports which appeared to name Customer 25 as a person involved in lower threshold financial crime; and

m. by reason of the matters set out at subparagraphs a. to l. above, there were real risks that Customer 25's source of wealth and source of funds were not legitimate.

Monitoring of Customer 25's transactions

1302. At no time did Crown Melbourne appropriately monitor Customer 25's transactions on a risk-basis.

Particulars

Section 36(1)(a), (b) of the Act and rules 15.4 to 15.8 of the Rules.

Crown Melbourne was unable to monitor the ML/TF risks posed by Customer 25's transactions appropriately because it did not make and keep appropriate records of designated services provided to junket players: see paragraphs 483 and 485.

Crown Melbourne did not apply appropriate risk-based transaction monitoring to designated services provided to Customer 25: see paragraphs 590ff, 629 to 642 and 643 to 649.

Customer 25 engaged in transactions indicative of ML/TF typologies and vulnerabilities such as refining: see particulars to paragraph 1303. Had appropriate risk-based transaction monitoring been applied, high risk and suspicious transactions could have been identified earlier: see paragraphs 686 and 687.

Ongoing customer due diligence

1303. On and from October 2016, on multiple occasions, the provision of designated services to Customer 25 by Crown Melbourne raised red flags reflective of higher ML/TF risks as a result of Customer 25 and persons associated with him transacting with large amounts of cash and cash that appeared suspicious, often in connection with Customer 1 or the Suncity junket.

Particulars

See paragraphs 450, 451 and 491.

See paragraph 521ff.

On 26 October 2016, Customer 25 exchanged $411,900 in cash comprising $50 notes for $100 notes on behalf of Customer 1. Three of the $50 notes were determined to be counterfeit: SMR dated 27 October 2016. This transaction was indicative of the ML/TF typology of refining.

On 4 December 2017, an unidentified person suspected to be Customer 25 presented at the Suncity cash administration desk with $400,000 in cash comprised of $100 and $50 notes: SMR dated 4 December 2017.

On 18 December 2017, Customer 25 presented at the Suncity cash administration desk with $300,000 in cash, which he exchanged for gaming chips: SMR dated 18 December 2017.

On 16 January 2018, an unknown person presented at the Suncity cash administration desk with $90,000 in cash, which he exchanged for gaming chips. The unknown person had been seen with Customer 25: SMR dated 16 January 2018.

On 21 February 2018, Customer 25 presented at the Suncity cash administration desk with $250,000 in cash, which he left at the Suncity cash administration desk and left the room without any chips being provided to him. However, Customer 25 was showing significant losses under the Suncity junket program at the time: SMR dated 21 February 2018.

On 26 February 2018, a junket representative for the Suncity junket presented at the Suncity cash administration desk with a backpack containing $100 notes bundled into units of $10,000. Customer 25 was present at the time and Crown Melbourne suspected that the funds belonged to him. However, Customer 25 was showing significant losses under the Suncity junket program at the time: SMR dated 26 February 2018.

On 22 July 2018, Customer 25 made a cash withdrawal of $103,000. Less than 20 minutes later, Customer 25 made an account deposit of $50,000.

On 14 August 2018, Customer 25 presented $80,000 in cash to be deposited into the Suncity junket account. The cash was allegedly brought by Customer 25's personal assistant from an unknown money changer. Five $50 notes were found to be counterfeit and the balance, being $79,750, was deposited: SMR dated 14 August 2018.

On 26 February 2019, while a key player on a junket program, two other key players in the junket program presented at the Cage with a shopping bag containing $220,000 in cash comprised of $50 and $100 notes bundled with rubber bands into groups of 100 notes. The key players indicated that the funds were from Customer 25. Crown Melbourne were unable to determine the true source of the funds: SMR dated 26 February 2019.

1304. On and from 1 March 2016, on multiple occasions, the provision of designated services to Customer 25 by Crown Melbourne raised red flags reflective of higher ML/TF risks as a result of Customer 25 engaging in complex, unusually large transactions and unusual patterns of transactions which had no apparent economic or visible lawful purpose, often in connection with Customer 1 or the Suncity junket.

Particulars

See paragraphs 420ff and 456ff.

On 20 May 2016, Customer 25 received a telegraphic transfer from a third party unknown to Crown Melbourne: SMR dated 23 May 2016.

On 24 June 2016, Customer 1 transferred $400,000 and $200,000 to Customer 25.

On 23 November 2017, a Crown Melbourne patron sent a telegraphic transfer of $350,000 to Customer 25.

Between 14 November 2016 and 2 July 2018, Customer 25 transferred $1,365,000 to Customer 1.

1305. On and from 1 March 2016, on multiple occasions, the provision of designated services to Customer 25 by Crown Melbourne raised red flags reflective of higher ML/TF risks as a result of Customer 25's recorded individual and junket play which involved high turnover.

Particulars

See paragraph 477.

Individual gaming activity

Between 2016 and 2018, Crown Melbourne recorded Customer 25's individual rated gaming activity to be cumulative buy-in of $2,230,700 and cumulative loss of $103,895.

Junket activity

By December 2016, Crown Melbourne recorded Customer 25's junket activity to be a cumulative turnover of $17,671,350 with a cumulative loss of $508,647.

Between 1 October 2017 and 1 November 2018, Crown Melbourne recorded Customer 25's junket activity to be a cumulative turnover of $283,728,860 and HKD24,420,000 with a cumulative loss of $8,778,170 and HKD2,342,100. This included one Suncity junket program in January 2018 in which Customer 25 had a turnover in excess of $100,000,000 and another Suncity junket program in August 2018 in which Customer 25 had a turnover in excess of $167,000,000.

Between 1 January 2019 and 4 February 2019, Crown Melbourne recorded Customer 25's junket activity to be a cumulative loss of $500,000: SMR dated 4 February 2019.

1306. At no time did Crown Melbourne undertake appropriate risk-based customer due diligence with respect to Customer 25 with a view to identifying, mitigating and managing the ML/TF risks posed by the provision of designated services on and from 1 March 2016.

a. At no time did Crown Melbourne take appropriate steps to understand whether Customer 25's source of wealth/funds was legitimate.

b. At no time did Crown Melbourne take appropriate steps to identify or analyse the ML/TF risks of Customer 25's transactions or to consider whether they had a lawful purpose.

c. At no time did Crown Melbourne give appropriate consideration to whether large and high risk transactions should be processed.

d. At no time did senior management consider whether continuing the business relationship with Customer 25 was within Crown Melbourne's ML/TF risk appetite.

Particulars

Section 36(1)(a) of the Act.

The due diligence steps taken with respect to Customer 25 included:

- risk intelligence searches conducted by Crown Melbourne in respect of Customer 25 on 6 December 2016, 21 September 2017 5 February 2018, 22 November 2018, 31 January 2019 and 26 April 2019. The 31 January 2019 search returned a media report published on 10 November 2016 which alleged that Customer 25 had engaged in lower threshold financial crime;
- on 16 April 2018, due diligence was initiated by Crown Melbourne in respect of Customer 25 as a key player in the Suncity junket; and
- on 21 November 2018, the CTRM reviewed the information held by Crown Melbourne in respect of Customer 25 and requested a wealth report. On 27 November 2018, external provider requested additional details to assist with locating information for the wealth report including Customer 25's employment. Crown Melbourne did not have this information and the request for a wealth report was cancelled.

None of these steps were proportionate to the ML/TF risks reasonably posed by Customer 25 on and from 1 March 2016.

Enhanced customer due diligence

1307. Having formed a suspicion for the purposes of s41 of the Act, Crown Melbourne gave the AUSTRAC CEO SMRs with respect to Customer 25 on:

a. 23 May 2016;

b. 27 October 2016;

c. 1 September 2017;

d. 27 November 2017;

e. 4 December 2017;

f. 18 December 2017;

g. 16 January 2018;

h. 1 February 2018;

i. 21 February 2018;

j. 26 February 2018;

k. 1 March 2018;

l. 14 August 2018;

m. 4 February 2019; and

n. 26 February 2019.

Particulars

The SMRs reported Customer 25's annual individual and junket losses, telegraphic transfers from third parties, the presentation by Customer 25 of large amounts of cash including counterfeit notes, the presentation of large amounts of cash on Customer 25's behalf by other persons and the amount of cash Customer 25 was prepared to carry.

1308. On each occasion that Crown Melbourne formed a suspicion with respect to Customer 25 for the purposes of s41 of the Act, it was required to apply its ECDD program to Customer 25.

Particulars

Rule 15.9(3) of the Rules.

1309. Crown Melbourne did not carry out appropriate risk-based ECDD measures with respect to Customer 25 on each occasion that Crown Melbourne formed a suspicion with respect to Customer 25 for the purposes of s41 of the Act.

a. There are no records of ECDD being conducted following the lodgement of any of the SMRs except the SMR given to the AUSTRAC CEO on 1 February 2018: see paragraphs 664 and 685.

b. Appropriate risk-based steps were not taken to obtain or analyse information about Customer 25's source of wealth/funds: see paragraph 667.

c. Appropriate risk-based steps were not taken to analyse and monitor Customer 25's transactions – both past and future – including to understand their economic purpose: see paragraph 590 and 666.

d. At no time did senior management consider whether continuing the business relationship with Customer 25 was within Crown Melbourne's ML/TF risk appetite.

Particulars

Rules 15.9(3), 15.10(1)(c), (d), (2), (5) and (6) of the Rules.

After lodging the SMR on 1 February 2018, which reported losses by a number of key players from a Suncity junket including Customer 25, Crown Melbourne conducted a risk intelligence search in respect of Customer 25. This search alone was not an appropriate step to understand Customer 25's source of wealth/funds or whether that source was legitimate.

See particulars to paragraph 1306.

1310. By reason of the matters pleaded from paragraphs 1294 to 1309, on and from 1 March 2016, Crown Melbourne:

a. did not monitor Customer 25 in relation to the provision of designated services, with a view to identifying, mitigating and managing the ML/TF risks it reasonably faced; and

b. did not do so in accordance with rr 15.5 and 15.9 of the Rules.

1311. By reason of the matters pleaded at paragraph 1310, Crown Melbourne contravened s36(1) of the Act on and from 1 March 2016 with respect to Customer 25.

Particulars

Section 36(1) of the Act is a civil penalty provision: s36(2) of the Act.

Customer 26

1312. Customer 26 was a customer of Crown Melbourne from 9 June 1996 to 15 August 2019.

1313. From at least 13 December 2006 to August 2019, Crown Melbourne provided Customer 26 with designated services within the meaning of table 1 and table 3, s6 of the Act.

Particulars

Customer 26 was registered at Crown Melbourne on 9 June 1996.

On 1 January 2011, Crown Melbourne opened a DAB account and safekeeping account (AUD) for Customer 26.

Crown Melbourne issued Customer 26 with a WOL that was in place from 21 February 2019 to 8 March 2019.

Crown Melbourne recorded Customer 26's individual rated gaming activity between 2006 and 2015 to be a cumulative turnover of $218,860,000, buy-in of $20,064,336 with a loss of $1,408,362. Customer 26's buy-in and turnover increased significantly in and from 2012.

Crown Melbourne recorded Customer 26's individual rated gaming activity between 2016 and 2019 to be a cumulative turnover of $113,580,000, buy-in of $10,240,000 with a loss of $1,253,370.

On 15 August 2019, Crown Melbourne banned Customer 26 from attending its premises and issued an indefinite WOL.

1314. Customer 26 was a customer of Crown Perth from at least 29 December 2016 to 29 June 2020.

1315. From at least 29 December 2016, Crown Perth provided Customer 26 with designated services within the meaning of table 1 and table 3, s6 of the Act.

Particulars

On 8 June 2018, Crown Perth opened a DAB account and safekeeping account (AUD) for Customer 26.

Crown Perth recorded Customer 26's individual rated gaming activity from 2016 to 2019 to be a cumulative turnover: $3,154,600, cumulative buy-in of $115,600 with a cumulative loss of $118,748.

On 29 June 2020, Crown Perth issued Customer 26 with an NRL. From evidence given at the Perth Casino Royal Commission, it is apparent that Customer 26 was permitted to enter Crown Perth until early 2021.

See paragraph 120.

1316. Customer 26 was a registered junket representative at Crown Melbourne and Crown Perth for at least three junkets.

Particulars

Customer 26 was a representative for the Meg-Star junket and two other junkets.

The ML/TF risks posed by Customer 26

1317. By 1 March 2016, higher ML/TF risks were indicated by:

a. the nature and purpose of Customer 26's business relationship with Crown Melbourne and Crown Perth;

b. the nature of the transactions Customer 26 had been conducting at Crown Melbourne and Perth;

c. the suspicions Crown Melbourne itself had formed with respect to Customer 26; and

d. Customer 26's source of funds/wealth as the owner of a brothel.

Particulars

Section 36(1)(a), (b) of the Act and Chapter 15 of the Rules.

SMRs by 1 March 2016

By 1 March 2016, Crown Melbourne had given the AUSTRAC CEO 12 SMRs in relation to Customer 26 – on 7 June 2007, 19 October 2010, 5 April 2011, 30 August 2011, 8 November 2011, 29 November 2011, 22 May 2012, 27 June 2012, 29 June 2012, 18 December 2013, 27 March 2015 and 24 February 2016.

Each SMR reported similar repeated patterns of suspicions relating to Customer 26's wins and losses. The SMRs described Customer 26's rated gaming activity, large cash transactions, his transactions and associations with other Crown patrons, his address being a shop, increase in average bet and third party transactions. The grounds of suspicion were based on Customer 26's annual losses, the amount of cash Customer 26 was prepared to carry, transactions between accounts and in respect of third parties and Customer 26's increase in average bets.

Law enforcement agency inquiries

In 2012, 2013 and 2014, law enforcement agencies requested that Crown Melbourne provide records and information relating to Customer 26 in connection with matters under the *Sex Work Act 1994* (Vic) and other criminal offences.

Other red flags

From 2011, media reports linked the brothel owned by Customer 26 to serious organised crime.

From 2014, the brothel regulator had commenced tribunal proceedings against Customer 26, alleging he was engaged in human trafficking.

From 2015, open court records reported that Customer 26's brothel had links to organised crime and serious criminal activity.

By 1 March 2016, neither Crown Melbourne nor Crown Perth had conducted any enquiries regarding Customer 26's source of funds/wealth which would have revealed the publicly available information described above.

1318. As at 1 March 2016, Customer 26 should have been recognised by Crown Melbourne and Crown Perth as a high risk customer for the reasons pleaded at paragraph 1317.

1319. At all times on and from 1 March 2016, Customer 26 should have been recognised by Crown Melbourne and Crown Perth as a high risk customer by reason of the matters pleaded at paragraphs 1317, 1322, 1323, 1324, 1325, 1326, 1329 and 1332.

Particulars

Section 36(1)(a), (b) of the Act and Chapter 15 of the Rules.

1320. It was not until 1 August 2019 that Crown Melbourne assessed Customer 26 as high risk.

Particulars

On various occasions between 7 June 2007 and 1 August 2019, Crown Melbourne assessed Customer 26's risk on at least 26 occasions and rated him as moderate or significant risk.

This was despite having received numerous requests for information from law enforcement agencies in relation to Customer 26, and despite lodging numerous SMRs.

It was not until 1 August 2019 that Crown Melbourne assessed Customer 26's risk as high. On various occasions between 1 August 2019 and 21 July 2021, Crown Melbourne assessed Customer 26's risk as high.

1321. It was not until 20 January 2021 that Crown Perth assessed Customer 26 as high risk.

Particulars

Crown Perth first assessed Customer 26's risk on 29 May 2019 and rated him as low risk.

Customer 26 was assessed and rated high risk by Crown Perth on 20 January 2021, 2 July 2021 and 21 July 2021.

At no point in time did Crown Perth assess Customer 26 as moderate or significant risk.

1322. On and from 1 March 2016, designated services provided to Customer 26 posed higher ML/TF risks to Crown Melbourne and Crown Perth, including because the provision of designated services to Customer 26 involved a combination of the following factors:

a. Customer 26 received high value financial (table 1, s6) and gaming services (table 3, s6);

b. Customer 26 was a junket representative for a number of junkets, including the Meg-Star junket;

c. by 2019, Crown Melbourne recorded Customer 26's individual rated gaming activity as a cumulative turnover exceeding $332,440,000;

d. by 2019, Crown Perth recorded Customer 26's individual rated gaming activity as a cumulative turnover exceeding $3,150,000;

e. designated services provided to Customer 26 involved large transfers to third parties, including to junket operators, including in connection to the Suncity junket;

f. large values were transferred to and from Customer 26's bank accounts and his DAB account, and to and from other customers' DAB accounts, involving the provision by Crown Melbourne of designated services within the meaning of items 31 and 32, table 1, s6 of the Act: see paragraphs 411ff and 492;

g. Customer 26 transacted using large amounts of cash and cash that appeared suspicious: see paragraphs 450, 451 and 452;

h. Customer 26 engaged in other transactions indicative of ML/TF typologies and vulnerabilities, including of structuring: see paragraph 24;

i. Customer 26 owned a brothel;

j. in 2014, Crown Melbourne became aware that Customer 26 was a person of interest to a law enforcement agency in connection with allegations of human trafficking, the operation of illegal brothels and the use of Crown Melbourne for the purpose of money laundering;

k. Crown Melbourne received multiple requests for information from law enforcement agencies in relation to Customer 26;

l. in 2015, open source court records relating to a fraud prosecution named Customer 26 as giving a person $100,000 in Crown gaming chips on the basis that person would transfer $100,000 to a third party;

m. Crown Melbourne failed to make appropriate enquiries as to Customer 26's source of funds/wealth. It was not until July 2019 that Crown Melbourne became aware that Customer 26 owned a brothel:

    i. from 2011, media reports linked the brothel to serious organised crime, including human trafficking and sex slavery;

    ii. in 2014, a brothel regulator launched action against Customer 26 before a tribunal alleging he was involved in human trafficking;

    iii. from 2015, open source court records reported that the brothel had links to organised crime and serious criminal activity, including money laundering; through the recruiting of women from a foreign region to work in the brothel for the material benefit of managers and staff;

    iv. from at least July 2019, media reports connected Customer 26 to the brothel and organised crime and serious criminal activity, including money laundering and the recruitment of women from foreign countries to work in the brothel for the material benefit of Customer 26; and

n. by reason of the matters pleaded at paragraphs a. to m. above, there were real risks that Customer 26's source of wealth and source of funds were not legitimate.

Monitoring of Customer 26's transactions

1323. At no time did Crown Melbourne or Crown Perth appropriately monitor Customer 26's transactions on a risk-basis.

Particulars

Section 36(1)(a), (b) of the Act and rules 15.4 to 15.8 of the Rules.

Crown Melbourne and Crown Perth were unable to monitor the ML/TF risks posed by Customer 26's transactions appropriately because they did not make and keep appropriate records of designated services provided to junkets and transactions involving junkets: see paragraphs 483ff.

Crown Melbourne and Crown Perth did not apply appropriate risk-based transaction monitoring to designated services provided to Customer 26: see paragraphs 590ff, 629 to 642 and 643 to 649.

Customer 26's transactions involved repeated transactions indicative of ML/TF typologies and vulnerabilities that were not detected prior to a 2021 lookback. Had appropriate risk-based transaction monitoring been applied, these transactions could have been identified earlier: see paragraphs 686 and 687.

In July 2021, Crown Melbourne identified transactions conducted by Customer 26 between 2010 and 2021 that were indicative of ML/TF typologies, including typologies related to structuring, large amounts of cash, cheques, and third party transfers.

In July 2021, Crown Perth identified transactions conducted by Customer 26 between 2010 and 2021 that were indicative of ML/TF typologies, including typologies related to cash, structuring and chip cash-outs.

Ongoing customer due diligence

1324. On and from 1 March 2016, on multiple occasions, the provision of designated services by Crown Melbourne and Crown Perth to Customer 26 raised red flags reflective of higher ML/TF risks by reason of Customer 26's involvement in complex, unusual large transactions and unusual patterns of transactions which had no apparent economic or visible lawful purpose.

Particulars

See paragraphs 420ff, 450, 451, 477 and 491.

Crown Melbourne

On 22 November 2016 Crown Melbourne received a transfer of $156,224 from another Australian casino for Customer 26, $150,000 of which Customer 26 transferred to an account associated with the Suncity junket, despite the fact that Customer 26 was not playing, nor had he recently played, on any program with the Suncity junket: SMR dated 23 November 2016.

On 14 January 2018, Customer 26 took a sum of cash in excess of $687,550 from the Suncity cash administration desk and gave that sum to Customer 22: SMR dated 15 January 2018.

On 21 February 2019, Crown Melbourne issued Customer 26 with a WOL as a result of several attempts to bring excluded patrons into the Mahogany Room and his history of abusing employees when asked for his card at the door or when signing in guests.

On 8 March 2019, Crown Melbourne lifted Customer 26's WOL.

Crown Perth

On and from 2018, Customer 26's turnover at Crown Perth started to increase, with a significant increase in 2019.

In April 2019, Customer 26 made successive transactions on his DAB account at Crown Perth for $6,700 and $5,000, indicative of structuring.

On 28 May 2019, Customer 26 cashed out $13,610 of chips in the Pearl Room, which did not correspond to his recorded play (a win of $5,000). Crown Perth gave the AUSTRAC CEO an SMR in respect of this conduct on 29 May 2019 and rated Customer 26's risk as low.

1325. From July 2019, the provision of designated services by Crown Melbourne and Crown Perth to Customer 26 raised red flags reflective of higher ML/TF risks as a result of media reports identifying Customer 26 as a person implicated in sex trafficking and organised crime.

Particulars

In July 2019, a journalist contacted Crown Melbourne requesting a comment on a proposed story. The journalist advised that he was examining whether Crown wilfully or recklessly breached foreign laws in relation to gambling and partnered with junkets with ties to serious organised crime. The journalist's asked whether Crown was aware of public allegations that Customer 26 owned brothels which were linked to illegal prostitution dating back to 1998 and human trafficking.

In July 2019, media articles were published reporting that Customer 26 was a business partner of Person 41, that Customer 26 was a Melbourne brothel owner allegedly implicated in sex trafficking and that his brothels had been named in court proceedings in connection with organised crime and the trafficking of sex workers from a foreign region to Melbourne. A media segment aired on the same day.

In July 2019, media articles were published reporting that Customer 26 was a junket operator at Crown Melbourne who would 'lure' foreign VIPs to Crown and was paid a commission, that Customer 26 was a junket representative and that foreign sex workers had been flown to Australia on the same flights used to transport Crown customers to Melbourne.

1326. The provision of designated services by Crown Melbourne and Crown Perth to Customer 26 raised red flags reflective of higher ML/TF risks as a result of Customer 26 being a person of

interest in law enforcement investigations, as identified by the Victorian Casino Operator and Licence Royal Commission.

Particulars

Victorian Casino Operator and Licence Royal Commission

In June and July 2021, a number of witnesses gave evidence relating to Customer 26 at the Victorian Casino Operator and Licence Royal Commission:

- a police officer identified Customer 26 as associated with an individual who was described as a prolific drug trafficker and affiliated with the illegal sex industry and "the point of source for the flow of money back [to Crown]";
- Customer 26 was described as a suspected member of an international organised crime group who associated with junket operators and junket representatives at Crown and other casinos;
- Customer 26 was identified as linked to Person 41 and Customer 46, each of whom were assessed by law enforcement to be involved in laundering money for serious organised crime groups; and
- Customer 26 was identified as a person of interest to a law enforcement agency, who had made inquiries with Crown in relation to Customer 26.

1327. At no time did Crown Melbourne undertake appropriate risk-based customer due diligence with respect to Customer 26 with a view to identifying, mitigating and managing the ML/TF risks posed by the provision of designated services on and from 1 March 2016.

a. At no time did Crown Melbourne take appropriate steps to understand whether Customer 26's source of wealth/funds was legitimate.

b. At no time did Crown Melbourne take appropriate steps to identify or analyse the ML/TF risks of Customer 26's transactions or to consider whether they had a lawful purpose.

c. At no time did Crown Melbourne give appropriate consideration to whether large and high risk transactions should be processed.

d. Prior to the decision to issue Customer 26 with a WOL in August 2019, there is no record of senior management considering whether continuing the business relationship with Customer 26 was within Crown Melbourne's ML/TF risk appetite in light of the ML/TF risks posed by Customer 26.

Particulars

Section 36(1)(a) of the Act.

There are no records of due diligence being conducted in respect of Customer 26 prior to July 2019, when Crown Melbourne was contacted by the media. This was not proportionate to the ML/TF risk reasonably posted by Customer 26 on and from 1 March 2016.

In late July 2019, Customer 26's patron information data and activity summary were circulated along with the results from risk intelligence and media report searches.

It was identified that there were no law enforcement inquiries on file.

Around 31 July 2019, Customer 26 was referred to Crown Melbourne's POI Committee. The POI Committee meeting agenda included the following:

- Customer 26 had first come to Crown's notice on 8 August 2006 and was Crown not aware of any allegations prior to the July 2019 media articles;
- Crown had received one request for records or information from a law enforcement agency and three requests for records or information from a second law enforcement agency. Crown had no knowledge of charges or convictions;
- risk intelligence searches and media report searches yielded no results;
- two cases related to Customer 26 before the County Court of Victoria: the first related to a third party obtaining property by deception, being $100,000 in cash from Customer 26 in connection with gaming chips, and the second related to money laundering by people involved with Customer 26's brothel; and
- under the heading 'media', quotes were extracted from a person who ran Customer 26's South Melbourne brothel who was recorded making admissions in an interview with a law enforcement agency's investigators, including that she had helped organise the recruitment of women in a foreign region to travel to Australia for the purpose of sex work with the full knowledge and permission of Customer 26. In 2014, a brothel regulator launched action against Customer 26 before a tribunal in an attempt to link him to human trafficking. Conditions on his brothel licence were added.

On about 1 August 2019, Crown Melbourne's legal team recommended that Crown Melbourne should ban Customer 26 because he was the sole director, secretary and shareholder of a company with principal place of business being the business address of the brothel where money laundering occurred per the County Court of Victoria case, together with comments of law enforcement in those matters.

The recommendation was supported by all senior management with the exception of one who opposed the recommendation on a number of grounds, including that were a great number of customers who Committee members may have heard allegations in respect of, which might in fact be true, but that cannot be substantiated.

On 14 August 2019, the POI Committee determined to issue a WOL in respect of Customer 26.

On 15 August 2019, Crown Melbourne banned Customer 26 from attending its premises and issued an indefinite WOL.

On 2 October 2020, the VCGLR served a show cause notice on Crown Melbourne under s20(2) of the *Casino Control Act 1991* (Vic). One of the allegations made by the VCGLR was that Crown Melbourne failed to identify issues in relation to Customer 26, who was alleged to be associated with a legal brothel that had been prosecuted for breaches of Victoria's sex workers laws and suspected to be involved in and have links to serious organised crime, in circumstances where two law enforcement agencies had notified Crown Melbourne about Customer 26's possible links to human trafficking, illegal brothels and money laundering. The show cause notice also referred to other individuals, including Customer 1, Customer 2 and Customer 32. On 27 April 2021, the VCGLR concluded that Crown Melbourne had breached s121(4) of the *Casino Control Act 1991* (Vic) and imposed a fine of $1,000,000.

Customer 26 was reviewed as part of the SPR process (see particulars to paragraph 1234) carried out between 2020 and 2021 and his licence to enter Crown Melbourne was withdrawn (notwithstanding that Customer 26 was already the subject of a WOL).

1328. At no time did Crown Perth undertake appropriate risk-based customer due diligence with respect to Customer 26 with a view to identifying, mitigating and managing the ML/TF risks posed by the provision of designated services on and from 1 March 2016.

a. At no time did Crown Perth take appropriate steps to understand whether Customer 26's source of wealth/funds was legitimate.

b. At no time did Crown Perth take appropriate steps to identify or analyse the ML/TF risks of Customer 26's transactions or to consider whether they had a lawful purpose.

c. At no time did Crown Perth give appropriate consideration to whether large and high risk transactions should be processed.

d. Prior to the decision to issue Customer 26 with an NRL in June 2020, there is no record of senior management considering whether continuing the business relationship with Customer 26 was within Crown Perth's ML/TF risk appetite in light of the ML/TF risks posed by Customer 26.

e. Although Crown Melbourne banned Customer 26 from attending its premises and issued an indefinite WOL on 15 August 2019, Customer 26 was permitted to enter Crown Perth at least 29 times after that date, as no cross-property barring system was in place. From evidence given at the Perth Casino Royal Commission, it is apparent that Customer 26 was permitted to enter Crown Perth until early 2021.

Particulars

Section 36(1)(a) of the Act.

There are no records of due diligence being conducted on Customer 26 by Crown Perth.

This was not proportionate to the ML/TF risk reasonably posted by Customer 26 on and from 1 March 2016.

On 29 June 2020, Crown Perth issued Customer 26 with an NRL.

Enhanced customer due diligence

1329. Having formed a suspicion for the purposes of s41 of the Act, Crown Melbourne gave the AUSTRAC CEO SMRs with respect to Customer 26 on:

a. 24 February 2016;

b. 23 November 2016;

c. 16 December 2016;

d. 15 January 2018;

e. 1 April 2019;

f. 30 July 2019; and

g. 1 July 2021.

Particulars

The SMRs reported Customer 26's annual losses and the amount of cash that Customer 26 was prepared to carry.

The SMR dated 1 July 2021 stated that Customer 26 had been a junket representative acting on behalf of Person 22, noted open source articles which showed that Customer 26 operated a brothel which was raided by a law enforcement agency on multiple occasions for sex trafficking concerns and that he had been accused of sex trafficking and money laundering and summarised all financial transactions it had recorded in relation to Customer 26 at both Crown Perth and Crown Melbourne.

1330. On each occasion that Crown Melbourne formed a suspicion with respect to Customer 26 for the purposes of s41 of the Act, it was required to apply its ECDD program to Customer 26.

Particulars

Rule 15.9(3) of the Rules.

1331. Crown Melbourne did not carry out appropriate risk-based ECDD measures with respect to Customer 26 on each occasion that Crown Melbourne formed a suspicion with respect to Customer 26 for the purposes of s41 of the Act.

a. There are no records of ECDD being conducted following the lodgement of SMRs on 23 November 2016, 15 January 2018 and 1 April 2019: see paragraphs 664 and 685.

b. Appropriate risk-based steps were not taken to obtain or analyse information about Customer 26's source of wealth/funds: see paragraph 667.

c. Appropriate risk-based steps were not taken to analyse and monitor Customer 26's transactions – both past and future – including to understand their economic purpose: see paragraph 590 and 666.

d. Prior to the decision to issue Customer 26 with a WOL in August 2019, there is no record of senior management considering whether continuing the business relationship with Customer 26 was within Crown Melbourne's ML/TF risk appetite in light of the ML/TF risks posed by Customer 26.

Particulars

Rules 15.9(3), 15.10(1)(c), (d), (2), (5) and (6) of the Rules.

See particulars to paragraph 1327.

1332. Having formed a suspicion for the purposes of s41 of the Act, Crown Perth gave the AUSTRAC CEO SMRs with respect to Customer 26 on:

a. 29 May 2019; and

b. 2 July 2021.

Particulars

The SMR dated 29 May 2019 reported Customer 26 cashing chips that did not correspond to his recorded play.

The SMR dated 2July 2021 stated that Customer 26 had been a junket representative acting on behalf of Person 22, noted open source articles which showed that Customer 26 operated a brothel which was raided by a law enforcement agency on multiple occasions for sex trafficking concerns and that he had been accused of sex trafficking and money laundering and summarised all financial transactions it had recorded in relation to Customer 26 at both Crown Perth and Crown Melbourne.

1333. On each occasion that Crown Perth formed a suspicion with respect to Customer 26 for the purposes of s41 of the Act, it was required to apply its ECDD program to Customer 26.

Particulars

Rule 15.9(3) of the Rules.

1334. Crown Perth did not carry out appropriate risk-based ECDD measures with respect to Customer 26 on each occasion that Crown Perth formed a suspicion with respect to Customer 26 for the purposes of s41 of the Act.

a. There are no records of ECDD being conducted following the lodgement of SMRs on 29 May 2019 or 2 July 2021: see paragraphs 664 and 685.

b. Appropriate risk-based steps were not taken to obtain or analyse information about Customer 26's source of wealth/funds: see paragraph 667.

c. Appropriate risk-based steps were not taken to analyse and monitor Customer 26's transactions – both past and future – including to understand their economic purpose: see paragraph 590 and 666.

d. Prior to the decision to issue Customer 26 with an NRL in June 2020, there is no record of senior management considering whether continuing the business relationship with Customer 26 was within Crown Perth's ML/TF risk appetite in light of the ML/TF risks posed by Customer 26.

Particulars

Rules 15.9(3), 15.10(1)(c), (d), (2), (5) and (6) of the Rules.

See particulars to paragraph 1328.

1335. On and from 1 August 2019, Crown Melbourne rated Customer 26 high risk.

Particulars

Crown Melbourne rated Customer 26 high risk on various occasions between 1 August 2019 and 21 July 2021: see paragraph 1320.

1336. On and from 20 January 2021, Crown Perth rated Customer 26 high risk.

Particulars

Crown Perth rated Customer 26 high risk on three occasions between 20 January 2021 and 21 July 2021: see paragraph 1321.

1337. On each occasion that Crown Melbourne or Crown Perth rated Customer 26 high risk, Crown Melbourne or Crown Perth was required to apply its ECDD program to Customer 26.

Particulars

Rule 15.9(1).

1338. Crown Melbourne and Crown Perth did not carry out appropriate risk-based ECDD measures with respect to Customer 26 on each occasion that Crown Melbourne and Crown Perth rated Customer 26 high risk.

Particulars

See particulars to paragraphs 1327, 1328, 1331 and 1334.

1339. By reason of the matters pleaded from paragraphs 1312 to 1338, on and from 1 March 2016, Crown Melbourne and Crown Perth:

a. did not monitor Customer 26 in relation to the provision of designated services, with a view to identifying, mitigating and managing the ML/TF risks it reasonably faced; and

b. did not do so in accordance with rr 15.5 and 15.9 of the Rules.

1340. By reason of the matters pleaded at paragraph 1339, Crown Melbourne contravened s36(1) of the Act on and from 1 March 2016 to August 2019 with respect to Customer 26.

Particulars

Section 36(1) of the Act is a civil penalty provision: s36(2) of the Act.

1341. By reason of the matters pleaded at paragraph 1339, Crown Perth contravened s36(1) of the Act on and from 1 March 2016 to 2021 with respect to Customer 26.

Particulars

Section 36(1) of the Act is a civil penalty provision: s36(2) of the Act.

Customer 27

1342. Customer 27 was a customer of Crown Melbourne from at least July 2008 to October 2009 and from June 2017.

1343. From at least July 2008 to October 2009 and from June 2017, Crown Melbourne provided Customer 27 with designated services within the meaning of table 1 and table 3, s6 of the Act.

Particulars

On 17 July 2008, Crown Melbourne opened a DAB account and safekeeping account (AUD) for Customer 27.

On 20 July 2008, Crown Melbourne opened a credit facility (AUD) for Customer 27.

Between 2007 and 22 July 2008, Customer 27 had a cumulative loss of $50,019,545.

From 21 October 2009, Customer 27 was issued with a WOL which was revoked on 15 June 2017.

On 22 May 2010, Crown Melbourne closed a credit facility account (AUD) for Customer 27.

1344. From at least 19 July 2008, Customer 27 received designated services as a junket player, facilitated through at least four different junket operators.

Particulars

Customer 27 received designated services through the Customer 2, Meg-Star and Suncity junkets and one other junket.

Between 1 February 2018 and 28 February 2018, Customer 27 was a key player in a Suncity junket program. Crown Melbourne recorded a junket loss in respect of Customer 27 of $14,943,000.

The ML/TF risks posed by Customer 27

1345. At all times from 1 March 2016, Crown Melbourne rated Customer 27 high risk.

Particulars

On various occasions between 27 October 2009 and 16 February 2021, Crown Melbourne assessed Customer 27 high risk.

See paragraph 481.

1346. By 21 October 2009, Crown Melbourne was on notice that Customer 27 had been taken into custody in a foreign country in connection with allegations of contract fraud.

Particulars

On 21 October 2009, Crown Melbourne had become aware that Customer 27 was taken into custody in a foreign country in May 2009 in connection with allegations of contract fraud and issued Customer 27 with a WOL.

In 2014, Customer 27 was sentenced to three years' imprisonment in connection with allegations of contract fraud.

The WOL was revoked on 15 June 2017.

1347. By 1 March 2016, higher ML/TF risks were indicated by the nature and purpose of Customer 27's business relationship with Crown Melbourne, the nature of the transactions he had been conducting, together with the suspicions Crown Melbourne itself had formed with respect to Customer 27.

Particulars

Section 36(1)(a), (b) of the Act and Chapter 15 of the Rules.

Customer 27 was a junket player. He received designated services through the channel of junket programs. This channel lacked transparency: see paragraph 477.

By 1 March 2016, Crown Melbourne had given the AUSTRAC CEO four SMRs in relation to Customer 27 – on 8 May 2007, 14 May 2007, 31 August 2007 and 21 July 2008. Each SMR reported annual losses and transactions between patron accounts, including between Customer 27 and his assistant and between Customer 27 and a junket operator.

On 19 July 2008, Customer 27 received a telegraphic transfer of a large sum in a foreign currency which he immediately transferred to a junket operator. That junket operator then transferred the funds to a second junket operator.

Customer 27 had significant individual losses at Crown Melbourne, being $40,059,045 in 2007 and $9,960,500 to 22 July 2008.

In 2014, Crown Casino brought proceedings against Customer 27 over his default on payment of a $10,000,000 debt.

1348. On and from 1 March 2016 designated services provided to Customer 27 posed higher ML/TF risks including because the provision of designated services to Customer 27 involved a combination of the following factors:

a. Customer 27 received high value financial (table 1, s6) and gaming services (table 3, s6) provided through multiple junket programs: see paragraph 473ff;

b. Customer 27 was a junket player;

c. Crown Melbourne issued Customer 27 with a WOL in 2009. The WOL was revoked on 15 June 2017 at which point Customer 27 was able to return to Crown Melbourne;

d. between 1 February 2018 and 28 February 2018, Customer 27 was a key player in a Suncity junket program and experienced a loss of $14,943,000;

e. designated services provided to Customer 27 involved a lack of transparency as the services were provided through the channel of junket programs, including the Suncity junket: see paragraph 521ff;

f. designated services provided to Customer 27 involved large transfers from third parties including junket operators and the cross-border movements of funds: see paragraph 239;

g. these transactions took place against the following background:

i. by 21 October 2009, Crown Melbourne was aware that Customer 27 had been taken into custody in a foreign country in connection with allegations of contract fraud;

ii. four SMRs being given to the AUSTRAC CEO by Crown Melbourne by 1 March 2016;

h. by 15 June 2017, Crown Melbourne were aware that Customer 27 had been found guilty of contract fraud and sentenced to three years' imprisonment, suspended for five years and fined. Crown Melbourne nonetheless revoked the WOL it has issued in respect of Customer 27; and

i. by reason of the matters set out at subparagraphs a. to h. above, there were higher ML/TF risks associated with Customer 27's source of wealth/funds.

Monitoring of Customer 27's transactions

1349. At no time did Crown Melbourne appropriately monitor Customer 27's transactions on a risk-basis.

Particulars

Section 36(1)(a), (b) of the Act and rules 15.4 to 15.8 of the Rules.

Crown Melbourne was unable to monitor the ML/TF risks posed by Customer 27's transactions appropriately because it did not make and keep appropriate records of designated services provided to junket players: see paragraphs 483ff.

Crown Melbourne did not apply appropriate risk-based transaction monitoring to designated services provided to Customer 27: see paragraphs 590ff, 629 to 642 and 643 to 649.

Ongoing customer due diligence

1350. On 15 June 2017, despite the higher ML/TF risks on and from 1 March 2016 pleaded at paragraphs 1346, 1347 and 1348, Crown Melbourne revoked the WOL issued in respect of Customer 27.

Particulars

By 17 September 2016, Crown Melbourne were aware that in 2014 Customer 27 was sentenced to three years' imprisonment in connection with allegations of contract fraud.

On 8 June 2017, Crown Melbourne received a request from an agent of the Suncity junket that Customer 27 be allowed to return to Crown Melbourne. Customer 27 had an outstanding debt of $9,615,532 to Crown Melbourne. Customer 27's return was conditional on an agreed amount of his outstanding debt being paid.

By 15 June 2017, Crown Melbourne were aware that Customer 27 had been charged in a foreign country with contract fraud, been sentenced to three years' imprisonment, suspended

for five years and fined. Crown Melbourne were also aware that, if Customer 27 were allowed to return to Crown Melbourne, he would have to apply for an Australian visa which would include certain checks.

On 15 June 2017, Crown Melbourne revoked the WOL in respect of Customer 27. Crown Melbourne did not appropriately consider the ML/TF risks posed by Customer 27 when determining to revoke the WOL it issued in respect of him.

1351. On and from 15 June 2017, on multiple occasions, the provision of designated services to Customer 27 raised red flags reflective of higher ML/TF risks.

Particulars

See paragraphs 450, 451, 477 and 491.

On 19 and 20 June 2017, a third party made large cash deposits in a foreign currency into the Suncity Account desk in favour of Customer 27 at Crown Melbourne. The funds were exactly half of Customer 27's outstanding debt to Crown Melbourne. Deposit slips were provided to Crown Melbourne without prior notice. The depositor's identification and address were recorded. However, the funds were not credited to Crown Melbourne because the Suncity Account was terminated: see paragraph 423.

Between 1 February 2018 and 28 February 2018, Customer 27 was a key player in a Suncity junket program. Crown Melbourne recorded a junket loss in respect of Customer 27 of $14,943,000.

In April 2018, Crown Melbourne agreed to offset $4,800,000 of Customer 27's outstanding debt against a debt owed by Crown Melbourne to the Suncity junket operator, Customer 1. Customer 1 executed an authority directing that the funds that had been deposited into the Suncity Account, which had not been credited to Crown Melbourne due to the cancellation of the program, could be transferred to his Suncity account in satisfaction of the debt Crown Melbourne owed him. SYCO was updated to show that Customer 27's debt to Crown Melbourne had been discharged. No funds were transferred from the Suncity Account to Crown Melbourne. The board of Crown Resorts and Crown Melbourne were not briefed on the proposed arrangement with Suncity: see paragraph 423.

On 1 May 2018, a third party sent a large international funds transaction in a foreign currency to Customer 27's Crown Melbourne DAB account for the repayment of Customer 27's outstanding debt.

On 29 January 2019, Customer 27 received two telegraphic transfers of $209,498 and $235,229 respectively from a third party.

1352. At no time did Crown Melbourne undertake appropriate risk-based customer due diligence with respect to Customer 27 with a view to identifying, mitigating and managing the ML/TF risks posed by the provision of designated services on and from 15 June 2017.

a. At no time did Crown Melbourne take appropriate steps to understand whether Customer 27's source of wealth/funds was legitimate. While Crown Melbourne were aware by June 2017 that Customer 27 was a property developer, they did not take appropriate steps to verify his source of wealth/funds.

b. At no time did Crown Melbourne take appropriate steps to identify or analyse the ML/TF risks of Customer 27's transactions or to consider whether they had a lawful purpose.

c. With the exception of the 19 and 20 June 2017 deposits at the Suncity Account, Crown Melbourne gave no consideration at any time to whether large and high risk transactions should be processed.

d. On 15 June 2017, senior management considered whether a business relationship with Customer 27 was within Crown Melbourne's ML/TF risk appetite and determined that Crown Melbourne would recommence a business relationship with Customer 27 despite the ML/TF risk that he posed.

e. After June 2017, at no time did senior management consider whether continuing the business relationship with Customer 27 was within Crown Melbourne's ML/TF risk appetite.

Particulars

Section 36(1)(a) of the Act.

The due diligence steps taken with respect to Customer 27 included:

In September 2016 and June 2017, Crown Melbourne obtained a wealth report in respect of Customer 27.

In June 2017, Crown Melbourne conducted a risk intelligence search in respect of Customer 27.

Senior management decision to revoke WOL in respect of Customer 27

In June 2017, the Senior Vice President (International Business) asked the Group General Manager (Regulatory and Compliance) to conduct a review in respect of Customer 27 to determine whether he could be accepted back at Crown Melbourne.

The Group General Manager (Regulatory and Compliance) confirmed that Customer 27 was a successful property developer, which was the source of his wealth, and that his WOL at Crown Melbourne was eight years old.

On 15 June 2017, a Manager (Compliance Reporting), sent an email to the Crown Melbourne POI Committee asking whether there were any concerns regarding the removal of stop codes in connection to Customer 27. That day, Crown Melbourne revoked the WOL in respect of Customer 27.

Crown Melbourne did not carry out any further due diligence in respect of Customer 27 after the WOL was revoked.

None of these steps were proportionate to the ML/TF risks reasonably posed by Customer 27 on and from 1 March 2016.

Enhanced customer due diligence

1353. Having formed a suspicion for the purposes of s41 of the Act, Crown Melbourne gave the AUSTRAC CEO SMRs with respect to Customer 27 on:

a. 1 March 2018; and

b. 2 May 2018.

Particulars

The SMR given to the AUSTRAC CEO on 1 March 2018 reported Customer 27's losses under the junket program and the amount of cash Customer 27 was prepared to carry.

The SMR given to the AUSTRAC CEO on 2 May 2018 reported third party telegraphic transfers involving Customer 27.

1354. On each occasion that Crown Melbourne formed a suspicion with respect to Customer 27 for the purposes of s41 of the Act, it was required to apply its ECDD program to Customer 27.

Particulars

Rule 15.9(3) of the Rules.

1355. Crown Melbourne did not carry out appropriate risk-based ECDD measures with respect to Customer 27 on each occasion that Crown Melbourne formed a suspicion with respect to Customer 27 for the purposes of s41 of the Act.

a. There are no records of ECDD being conducted following the lodgement of SMRs on 1 March 2018 or 2 May 2018: see paragraphs 664 and 685.

b. Appropriate risk-based steps were not taken to obtain or analyse information about Customer 27's source of wealth/funds: see paragraph 667.

c. Appropriate risk-based steps were not taken to analyse and monitor Customer 27's transactions – both past and future – including to understand their economic purpose: see paragraph 590 and 666.

d. On 15 June 2017, senior management considered whether a business relationship with Customer 27 was within Crown Melbourne's ML/TF risk appetite and determined that Crown Melbourne would recommence a business relationship with Customer 27 despite the ML/TF risk that he posed.

e. After June 2017, at no time did senior management consider whether continuing the business relationship with Customer 27 was within Crown Melbourne's ML/TF risk appetite.

Particulars

Rules 15.9(3), 15.10(1)(c), (d), (2), (5) and (6) of the Rules.

See particulars to paragraph 1352.

1356. On and from 1 March 2016, Crown Melbourne rated Customer 27 high risk.

Particulars

Crown Melbourne rated Customer 27 high risk on three occasions between 24 May 2017 and 21 May 2019: see paragraph 1345.

1357. On each occasion that Crown Melbourne rated Customer 27 high risk, Crown Melbourne was required to apply its ECDD program to Customer 27.

Particulars

Rule 15.9(1).

1358. Crown Melbourne did not carry out appropriate risk-based ECDD measures with respect to Customer 27 on each occasion that Crown Melbourne rated Customer 27 high risk.

Particulars

See particulars to paragraphs 1352 and 1355.

1359. By reason of the matters pleaded from paragraphs 1342 to 1358, on and from June 2017, Crown Melbourne:

a. did not monitor Customer 27 in relation to the provision of designated services, with a view to identifying, mitigating and managing the ML/TF risks it reasonably faced; and

b. did not do so in accordance with rr 15.5 and 15.9 of the Rules.

1360. By reason of the matters pleaded at paragraph 1359, Crown Melbourne contravened s36(1) of the Act on and from June 2017 with respect to Customer 27.

Particulars

Section 36(1) of the Act is a civil penalty provision: s36(2) of the Act.

Customer 28

1361. Customer 28 has been a customer of Crown Melbourne since 7 February 2000.

1362. From at least December 2006, Crown Melbourne provided Customer 28 with designated services within the meaning of table 1 and table 3, s6 of the Act.

1363. Customer 28 received designated services as a junket player, facilitated through six different junket operators.

Particulars to paragraphs 1362 and 1363

On 7 February 2000, Crown Melbourne opened a DAB account and safekeeping account (AUD) for Customer 28 under two PIDs.

On 7 August 2000, Customer 28 became a Crown premium program player.

Customer 28 received designated services under the Person 3, Person 21, Customer 6 and another junket program.

Between 2008 and 2017, Customer 28's total turnover on junket programs at Crown Melbourne was $337,600,000 with total losses of $13,670,000 and total wins of $3,005,050.

The ML/TF risks posed by Customer 28

1364. By 1 March 2016, higher ML/TF risks were indicated by the nature and purpose of Customer 28's business relationship with Crown Melbourne, the nature of the transactions he had been

conducting, together with the suspicions Crown Melbourne itself had formed with respect to Customer 28.

Particulars

Section 36(1)(a), (b) of the Act and Chapter 15 of the Rules.

Customer 28 was a junket player. He received designated services through the channel of junket programs. This channel lacked transparency: see paragraph 477.

By 1 March 2016, Customer 28's total turnover on junket programs at Crown Melbourne was $197,280,000 with total losses of $13,670,000 and total wins of $935,050.

By 1 March 2016, Crown Melbourne had given the AUSTRAC CEO six SMRs in relation to Customer 28. One SMR related to a transaction indicative of the ML/TF typology of structuring, involving the presentation of $10,000 in cash to purchase gaming chips, but only purchasing $9,900 in chips when asked to provide identification.

The remaining five SMRs related to suspicions formed by Crown Melbourne with respect to Customer 28's losses under junket programs, totalling $20,142,650 between June 2008 and December 2014. The SMR dated 9 October 2009 noted that following the completion of the junket program, the junket operator arranged for $2,000,000 to be transferred to Customer 28's overseas bank account, despite him having lost $4,918,200 under the program.

At no time prior to 1 March 2016 did Crown Melbourne take any due diligence steps with respect to Customer 28.

1365. As at 1 March 2016, Customer 28 should have been recognised by Crown Melbourne as a high risk customer for the reasons pleaded at paragraph 1364 and by reason of his PEP status pleaded in paragraph 1376.

Particulars

Section 36(1)(a), (b) of the Act and Chapter 15 of the Rules.

1366. At all times on and from 1 March 2016, Customer 28 should have been recognised by Crown Melbourne as a high risk customer by reason of the matters pleaded at paragraphs 1364, 1368, 1370, 1371, 1372, 1373, and 1376.

1367. It was not until 15 November 2017 that Customer 28 was rated high risk by Crown Melbourne.

Particulars

On various occasions between 10 June 2008 and 22 July 2016, Crown Melbourne assessed Customer 28 as moderate risk.

On various occasions between 15 November 2017 and 19 October 2018, Crown Melbourne assessed Customer 28 as high risk.

See paragraph 481.

1368. On and from 1 March 2016, designated services provided to Customer 28 posed higher ML/TF risks including because the provision of designated services to Customer 28 involved a combination of the following factors:

a. Customer 28 received high value financial (table 1, s6) and gaming services (table 3, s6) provided through multiple junket programs: see paragraph 473ff;

b. Customer 28 was a junket player;

c. Customer 28 was a foreign PEP: see paragraphs 118 and 663;

d. by no later than November 2017, Crown Melbourne recorded that Customer 28's total turnover on junket programs at Crown Melbourne had exceeded $337,680,000;

e. Customer 28 was known at all times to be connected to junket operators, including junket operators in respect of whom Crown Melbourne or Crown Perth had formed suspicions such as Customer 6 and Person 3, who were both connected to the Neptune junket;

f. designated services provided to Customer 28 lacked transparency as the services were provided through the channel of junket programs: see paragraph 477(e);

g. the table 3, s6, designated services provided to Customer 28 involved escalating rates of high turnover;

h. designated services provided to Customer 28 involved large transfers to and from third parties: see paragraph 456ff;

i. large values were transferred to Customer 28's DAB account from other customers' DAB accounts, involving the provision by Crown Melbourne of designated services within the meaning of items 31 and 32, table 1, s6 of the Act: see paragraphs 411ff and 492;

j. Customer 28 made or received large transfers and unusual requests for transfers to other overseas casinos, including Crown Aspinalls: see paragraphs 398ff and 407ff;

k. at various times, Customer 28 was provided with significant amounts of credit upon request, up to limits of GBP8,000,000, which was used to play on junket programs including at Crown Aspinalls: see paragraph 280ff;

l. Customer 28 incurred two separate debts to Crown, both of which were paid by third parties;

m. by November 2018, Customer 28 had significant parked or dormant funds in his DAB account: see paragraph 252;

n. these transactions took place against the background of:

    i. Customer 28 having engaged in transactions indicative of ML/TF typologies and vulnerabilities, including structuring the purchase of gaming chips to avoid providing identification: see paragraph 24; and

    ii. six SMRs being given to the AUSTRAC CEO by Crown Melbourne by 1 March 2016;

o. by 23 March 2017, Crown Melbourne was aware of open source articles naming Customer 28 as a person allegedly involved in money laundering, underground banking and other criminal activities; and

p. by reason of the matters set out at subparagraphs a. to o. above, there were real risks that Customer 28's source of wealth/funds were not legitimate.

Monitoring of Customer 28's transactions

1369. At no time did Crown Melbourne appropriately monitor Customer 28's transactions on a risk-basis.

Particulars

Section 36(1)(a), (b) of the Act and rules 15.4 to 15.8 of the Rules.

Crown Melbourne was unable to monitor the ML/TF risks posed by Customer 28's transactions appropriately because it did not make and keep appropriate records of designated services provided to junket players: see paragraphs 483ff.

Crown Melbourne did not apply appropriate risk-based transaction monitoring to designated services provided to Customer 28: see paragraphs 590ff, 629 to 642 and 643 to 649.

Ongoing customer due diligence

1370. From 2017, on multiple occasions, the provision of designated services to Customer 28 by Crown Melbourne raised red flags reflective of higher ML/TF risks arising from Customer 28's junket activity and unusual transactions at Crown Melbourne.

Particulars

See paragraphs 420ff and 477.

Between 31 October 2017 and 14 November 2017, Customer 28 attended Crown Melbourne as a player on a junket run by Customer 6. Crown Melbourne recorded that Customer 28's turnover on the program was $140,400,850, with losses of $2,065,250.

By 11 November 2018, Customer 28 held AU$20,217,282 in his safekeeping account.

On 14 May 2019, Customer 28 arranged for a large telegraphic transfer in a foreign currency to be sent from his Crown Melbourne DAB account to Crown Aspinalls.

1371. In 2017, Crown Melbourne received payments for debts owed by Customer 28 via the Suncity Account, which raised red flags reflective of higher ML/TF risks. The funds were deposited in the Suncity Account by a third party.

Particulars

On 27 July 2017, Customer 28 utilised the Suncity Account by arranging for an agent to deposit a large cash sum in a foreign currency to redeem the debt he owed to Crown Aspinalls.

See paragraphs 513 to 515.

1372. In 2018, the provision of designated services to Customer 28 by Crown Melbourne raised red flags reflective of higher ML/TF risks arising from Customer 28's use of a third party to repay a debt owed to Crown Melbourne.

Particulars

See paragraph 456ff.

On 29 June 2018, a third party, Person 6, transferred a large sum in a foreign currency to Crown Melbourne's account to be used to repay Customer 28's debt that he owed to Crown Aspinalls, which was received into the account on 2 July 2018.

On 15 August 2018, Person 6 transferred a further large sum in a foreign currency to Crown Melbourne's account, for the benefit of Customer 28.

On 30 August 2018, Person 6 transferred a large sum in a foreign currency from his Crown DAB account to Customer 28's Crown Melbourne safekeeping account.

On 19 September 2018, Person 6 transferred a large sum in a foreign currency by telegraphic transfer to Customer 28's DAB account at Crown Melbourne.

1373. On and from 1 March 2016, on multiple occasions, Crown Melbourne regularly approved credit that was used to fund Customer 28's junket activity at Crown Aspinalls, which involved high turnover and unusual transactions that ought to have raised red flags in relation to the provision of designated services to Customer 28.

Particulars

Between 21 July 2016 and at least 4 July 2017, Crown management regularly reapproved Customer 28's credit facility, up to limits of GBP3,000,000 and GBP8,000,000. Customer 28 used these funds to play on junkets at Crown Aspinalls.

In September 2017, Crown management approved a credit facility for another junket operator, Customer 6, up to a limit of GBP3,000,000. Customer 6's key players, including Customer 28, used these funds to play on Customer 6's junket at Crown Aspinalls.

Junket activity

Between 24 January 2017 and 28 January 2017, Customer 28 played at Crown Aspinalls. Crown Aspinalls recorded that Customer 28's total turnover for that program was GBP132,921,000 with wins of GBP12,055,440.

In May 2017, Customer 28 played at Crown Aspinalls. Crown Aspinalls recorded that Customer 28's total turnover for that program was GBP28,496,250 with losses of GBP3,495,750.

Between 19 September 2017 and 20 September 2017, Customer 28 attended Crown Aspinalls as a key player on a junket program run by Customer 6. Crown Aspinalls recorded that Customer 28's total turnover for that program was turnover of GBP40,805,500 and losses of GBP7,933,582.

1374. At no time did Crown Melbourne undertake appropriate risk-based customer due diligence with respect to Customer 28 with a view to identifying, mitigating and managing the ML/TF risks posed by the provision of designated services on and from 1 March 2016.

a. At no time did Crown Melbourne take appropriate steps to understand whether Customer 28's source of wealth/funds was legitimate.

b. At no time did Crown Melbourne take appropriate steps to identify or analyse the ML/TF risks of Customer 28's transactions or to consider whether they had a lawful purpose.

c. At no time did Crown Melbourne give appropriate consideration to whether large and high risk transactions should be processed.

d. At no time did senior management consider whether continuing the business relationship with Customer 28 was within Crown Melbourne's ML/TF risk appetite.

e. Despite Customer 28 being referred to the POI Committee in October 2021, the POI Committee had not reviewed Customer 28 by November 2021 and he was referred a second time.

Particulars

Section 36(1)(a) of the Act.

The due diligence steps taken with respect to Customer 28 included:

Database searches

On 21 July 2016, 20 October 2016, 24 January 2017, 15 November 2017, 26 April 2018, 19 October 2018, and 4 November 2021, Crown performed risk intelligence searches on Customer 28, which reported that Customer 28 was a foreign PEP due to his position as a member of a foreign political advisory body from March 2013.

On 21 July 2016, 5 January 2017, 23 March 2017, May 2017, and May 2018, Crown performed a series of searches on bankruptcy, company, and litigation databases, to obtain information on Customer 28.

On 23 March 2017, Crown also performed open source searches and obtained media reports on Customer 28 that alleged that he:

- operated an underground money lending business;
- held immunity from prosecution due to his high level political connections; and
- provided the son of a former foreign political leader and his wife with a property in Australia in exchange for being able to settle business deals in a foreign country.

At no point, as a result of these searches, did Crown Melbourne appropriately consider the ML/TF risks of the source of Customer 28's wealth/funds or whether an ongoing business relationship with Customer 28 was within its ML/TF risk appetite.

Wealth reports

On 21 June 2016, 23 March 2017 and 30 August 2021, Crown obtained wealth reports on Customer 28. The report dated 21 June 2016 disclosed that he allegedly made money through drug deals, prostitution and underground money lending.

Senior management engagement

On 23 March 2017, a Crown Aspinalls employee emailed the Senior Vice President (International Business) and the Group Credit Control Manager (VIP International) confirming that Crown Aspinalls was aware of the negative media on Customer 28, but it had determined there was no evidence to substantiate the allegations or any legal action taken.

On 15 November 2017, Crown Melbourne's CTRM identified Customer 28 as a foreign PEP, on the basis of the political position he had held since March 2013. The CTRM sought approval from the Chief Legal Officer (Australian Resorts) to continue a business relationship with the customer, which was granted.

On 19 October 2018, the Credit control team identified Customer 28 as an inactive PEP. The Senior Vice President (International Business) was informed of the same.

None of these steps were proportionate to the ML/TF risks reasonably posed by Customer 28 on and from 1 March 2016.

Significant Player Review

It was not until September 2021 that Crown Melbourne began to give consideration to whether Customer 28 was within Crown Melbourne's ML/TF risk appetite.

On 1 September 2021, Crown identified Customer 28 through its SPR process and performed further due diligence on Customer 28: see particulars to paragraph 1234.

On 25 October 2021, Customer 28 was given a risk rating of medium as a result of the SPR process and referred to the POI Committee for decision.

On 4 November 2021, after completing a KYC Table Games Subject Profile on Customer 28, a Crown employee again recommended that Customer 28's profile be referred to the POI Committee.

1375. Between 30 May 2012 and 10 October 2019, a number of widely accessible media and open source articles were published in respect of Customer 28. These articles do not appear to have come to Crown's attention as part of its due diligence process.

Particulars

The media reports concerned Customer 28's business and property associations with an individual who was the son of a former political leader.

Open source articles also alleged that Customer 28 was involved in money laundering through underground banks for foreign political officials and businessmen.

Enhanced customer due diligence

1376. At all times from 1 March 2016, Customer 28 was a foreign PEP.

Particulars

Section 36(1)(a) of the Act.

Customer 28 was a foreign PEP due to his position as a member of a foreign political advisory body from March 2013.

1377. At all times from 1 March 2016, Crown Melbourne was required to apply its ECDD program to Customer 28.

Particulars

Rules 15.9(2), 15.11 of the Rules

See paragraphs 660, 663 and 666.

1378. Crown Melbourne did not carry out appropriate risk-based ECDD measures with respect to Customer 28 on and from 1 March 2016 given his status as a foreign PEP. In particular:

a. Crown Melbourne did not undertake a detailed analysis of Customer 28's KYC information or analyse the legitimacy of Customer 28's source of wealth/funds;

b. on occasions where senior management approved a continuing business relationship with Customer 28 as a foreign PEP, senior management failed to give adequate consideration to the ML/TF risks posed by Customer 28 given his status as a foreign PEP; and

c. on occasions where senior management approved continuing to provide designated services to Customer 28 as a foreign PEP, management failed to give adequate consideration to the ML/TF risks posed by Customer 28 given his status as a foreign PEP.

Particulars

Rules 15.10(2), 15.10(6), 15.11 of the Rules.

See particulars to paragraph 1374.

See paragraph 660, 663, 666, 667 and 668.

1379. On and from 15 November 2017, Crown Melbourne rated Customer 28 high risk.

On various occasions between 15 November 2017 and 19 October 2018, Crown Melbourne assessed Customer 28 as high risk: see paragraph 1366.

1380. On each occasion that Crown Melbourne rated Customer 28 high risk, Crown Melbourne was required to apply its ECDD program to Customer 28.

Particulars

Rule 15.9(1).

1381. Crown Melbourne did not carry out appropriate risk-based ECDD measures with respect to Customer 28 on each occasion that Crown Melbourne rated Customer 28 high risk.

Particulars

At no time did Crown Melbourne conduct ECDD following each occasion that it rated Customer 28 high risk.

See particulars to paragraph 1374.

1382. By reason of the matters pleaded from paragraphs 1361 to 1381, on and from 1 March 2016, Crown Melbourne:

a. did not monitor Customer 28 in relation to the provision of designated services, with a view to identifying, mitigating and managing the ML/TF risks it reasonably faced; and

b. did not do so in accordance with rr 15.5 and 15.9 of the Rules.

1383. By reason of the matters pleaded at paragraph 1382, Crown Melbourne contravened s36(1) of the Act on and from 1 March 2016 with respect to Customer 28.

Particulars

Section 36(1) of the Act is a civil penalty provision: s36(2) of the Act.

Customer 29

1384. Customer 29 has been a customer of Crown Melbourne since 6 April 2007.

1385. Between February 2012 and 20 January 2021, Crown Melbourne provided Customer 29 with designated services within the meaning of table 1 and table 3, s6 of the Act.

Particulars

On 11 February 2012, Crown Melbourne opened a DAB account and safekeeping account (AUD) for Customer 29, which remain open. On 18 November 2016, Crown Melbourne opened a second DAB account and safekeeping account (AUD) for Customer 29, which remain open.

On 12 February 2012, Crown Melbourne opened a credit facility (AUD/HKD) for Customer 29 which was closed on 25 November 2016. On 18 November 2016, Crown Melbourne opened a second credit facility (AUD) for Customer 29 which was closed on 19 June 2021.

Between 2012 and 2013, Crown Melbourne recorded Customer 29's total individual rated gaming activity to be a cumulative buy-in of $69,043,775 with a cumulative loss of $17,012,853.

In 2017, Crown Melbourne recorded Customer 29's total individual rated gaming activity to be a win of $29,400.

In December 2018, Customer 29 travelled overseas and was unable to return due to the cancellation of his visa.

On 20 January 2021, Customer 29 was issued a WOL at Crown Melbourne as a result of the application of the SPR process: see particulars to paragraph 1234.

1386. From at least April 2010, Customer 29 received designated services as a junket player at Crown Melbourne, facilitated through four different junket operators.

Particulars

Customer 29 attended Crown Melbourne as a junket player on at least 52 occasions.

Customer 29 received designated services at Crown Melbourne through the Customer 51 and three other junkets (including the junkets of Person 42 and Person 44).

In 2013, Customer 29 had a junket turnover of $358,520,000.

In 2017 and 2018, this turnover had escalated to $1,881,320,000 and $1,673,550,000 respectively.

Crown Melbourne recorded Customer 29's total junket activity between 2013 and 2018 to be cumulative turnover of $6,122,190,000 with a cumulative loss of $14,777,770.

In December 2018, Customer 29 travelled overseas and was unable to return due to the cancellation of his visa.

1387. Customer 29 has been a customer of Crown Perth since 24 November 2011.

1388. From at least December 2011, Crown Perth provided Customer 29 with designated services within the meaning of table 1 and table 3, s6 of the Act.

Particulars

On 1 December 2011, Crown Perth opened a DAB account and safekeeping account (AUD/HKD) for Customer 29, which remains open. On 11 February 2012, Crown Perth opened a second DAB account and safekeeping account (AUD) for Customer 29, which remains open.

On 27 March 2012, Crown Perth opened a FAF account (AUD/HKD) for Customer 29 which was closed on 7 November 2016.

1389. From at least 4 June 2012, Customer 29 received designated services as a junket player at Crown Perth facilitated through one junket operator.

Particulars

Customer 29 received designated services at Crown Perth through Person 44's junket program.

By 24 April 2013, Crown Perth recorded Customer 29's individual gaming activity and gaming activity on junket programs to be a cumulative turnover of $421,110,215 with a loss of $8,718,370. Customer 29 was paid a commission of $2,526,668 by Crown Perth.

Between 14 October 2016 and 6 August 2017, a junket under which Customer 29 was the primary or sole key player recorded a turnover at Crown Perth of $310,000,000.

The ML/TF risks posed by Customer 29

1390. By 1 March 2016, higher ML/TF risks were indicated by the nature and purpose of Customer 29's business relationship with Crown Melbourne and Crown Perth, the nature of the transactions he had been conducting, together with the suspicions Crown Melbourne and Crown Perth itself had formed with respect to Customer 29.

Particulars

Section 36(1)(a), (b) of the Act and Chapter 15 of the Rules.

Customer 29 was a junket player. He received designated services through the channel of junket programs. This channel lacked transparency: see paragraph 477.

SMRs by 1 March 2016

By 1 March 2016, Crown Melbourne had given the AUSTRAC CEO 17 SMRs in relation to Customer 29 – on 14 February 2012, 15 February 2012, 16 February 2012, 25 May 2012, 19 July 2012, 27 December 2012, 27 May 2013, 1 July 2013, 10 October 2013, 8 November 2013, 4 December 2013, 6 December 2013, 1 May 2014, 12 June 2015, 28 August 2015, 2 November 2015 and 2 February 2016. The SMRs described concerns raised in respect of Customer 29's name and aliases, third party transactions, large annual individual and junket losses, wealth reports and the amount of cash Customer 29 was prepared to carry.

By 1 March 2016, Crown Perth had given the AUSTRAC CEO three SMRs in relation to Customer 29 – on 7 June 2012, 14 June 2012 and 10 July 2012. The SMRs described concerns raised in respect of Customer 29's name and aliases and telegraphic transfers of junket program winnings to third parties.

Transactions indicative of ML/TF typologies by 1 March 2016

Between December 2013 and April 2014, Customer 29 engaged in transactions that, in 2020, an independent auditor identified as indicative of ML/TF typologies involving transfers by overseas money remitters, including:

- on 9 December 2013, $270,000 received by Crown Melbourne for Customer 29 from a company account and $891,300.78 received from Company 2's account;
- on 10 December 2013, $390,658 received by Crown Melbourne for Customer 29 from a company account;
- on 30 December 2013, $1,822,489.52 received by Crown Melbourne for Customer 29 from Company 2's account; and

- on 10 April 2014, $857,632.93 received by Crown Melbourne for Customer 29 from Company 2's account.

On 11 June 2015, Customer 29 engaged in a transaction indicative of ML/TF typologies involving transfers by international third parties. $1,991,735 was received by Crown Melbourne for Customer 29 from a third party: SMR dated 12 June 2015.

Large and unusual transactions by 1 March 2016

By 1 March 2016, Customer 29 had been involved in many high value transactions to Crown patrons and third parties, including:

- on 14 February 2012, $107,624 sent by Crown Melbourne for Customer 29 to a third party: SMR dated 15 February 2012;
- on 26 March 2013, $1,347,208 transferred by Customer 29 to another Crown Melbourne patron Customer 51;
- on 5 December 2013, $1,373,000 received by Crown Melbourne for Customer 29 from a third party: SMR dated 6 December 2013;
- in 2014, a total of $10,894,115 sent from a junket operator, Person 44, to Customer 29's personal account;
- on 12 June 2015, $2,000,000 received by Crown Melbourne for Customer 29 from a third party: SMR dated 12 June 2015;
- on 27 August 2015, $605,810 sent by Crown Melbourne for Customer 29 to a third party: SMR dated 28 August 2015;
- on 30 October 2015, $7,711,162 received by Crown Melbourne for Customer 29 from a third party: SMR dated 2 November 2015; and
- in 2015, a total of $7,266,820 sent from a junket operator, Person 44, to Customer 29's personal account.

Other red flags by 1 March 2016

On 3 June 2012, Customer 29 provided to Crown Perth a blank cheque as security in respect of a program. The blank cheque used a name different to that on his passport. Crown Melbourne sent to Crown Perth a copy of the passport it had on file. That passport had the same name as the blank cheque provided to Crown Perth. The two passports had different names and birth years: SMR dated 7 June 2012.

On 1 August 2012, Crown Melbourne received a notice under the Act from a law enforcement agency in respect of Customer 29.

In 2012, on several occasions, Customer 29 requested that the balance of his Crown Perth and Crown Melbourne junket winnings be transferred to his wife: SMRs dated 15 February 2012, 14 June 2012 and 10 July 2012.

Due diligence conducted by June 2015

In April 2015, Crown Perth reviewed Customer 29's ML/TF risk level at a compliance officer meeting. Customer 29's risk rating at Crown Perth was decreased to low. There is no evidence of due diligence being conducted in respect of this review.

On 1 May 2015, Crown Melbourne prepared a patron credit profile in respect of Customer 29 and approved a credit limit of $5,000,000 with TTO of $10,000,000. A central credit report was obtained in connection with this patron credit profile for Customer 29 and his aliases.

Between 2013 and June 2015, Customer 29 had a cumulative turnover at Crown Melbourne in the range of a billion dollars and had been involved in many high-value telegraphic transfers indicative of ML/TF typologies. Other than the April 2015 review, no due diligence was conducted by Crown Melbourne in respect of Customer 29 in this period. It was a June 2015 media report that triggered due diligence to be conducted in respect of Customer 29.

The 2015 review

On 18 June 2015, Crown Melbourne conducted a political donation search, Australian company, property and risk intelligence searches in respect of Customer 29 and his company, Company 15.

1391. At all times, Customer 29 was a foreign PEP.

Particulars

In June 2015, Crown Melbourne obtained a wealth report in respect of Customer 29 that:

- identified Customer 29's aliases and high estimated net worth;
- identified that Customer 29 was a member of several foreign political organisations; and
- stated that Customer 29 may have fled to Australia to avoid arrest in connection with bribery charges involving the major of a city in a foreign country.

In July 2015, Crown Melbourne conducted a company search and obtained another wealth report in respect of Customer 29 that again identified Customer 29 as a foreign PEP.

Despite the two 2015 wealth reports, Customer 29 was not determined to be a foreign PEP by Crown Melbourne and Crown Perth until 2018.

1392. By 1 March 2016, Customer 29 should have been recognised by Crown Melbourne and Crown Perth as a high risk customer by reason of the matters pleaded at paragraph 1390 and by reason of his PEP status pleaded at paragraph 1391.

Particulars

Section 36(1)(a), (b) of the Act and Chapter 15 of the Rules.

1393. At all times on and from 1 March 2016, Customer 29 should have been recognised by Crown Melbourne and Crown Perth as a high risk customer by reason of the matters pleaded at paragraphs 1390, 1391, 1396, 1397, 0, 1400, 1401, 1402, 1404 and 1407.

Particulars

Section 36(1)(a), (b) of the Act and Chapter 15 of the Rules.

1394. It was not until 9 January 2018 that Customer 29 was rated high risk by Crown Melbourne.

Particulars

On various occasions between 14 February 2012 and 2 August 2012, Crown Melbourne rated Customer 29's risk as moderate.

On various occasions between 3 August 2012 (following a law enforcement inquiry) and 23 April 2014, Crown Melbourne rated Customer 29's risk as significant.

On various occasions between 24 April 2014 and 8 January 2018, Crown Melbourne rated Customer 29's risk as moderate.

This was despite Customer 29's turnover by 2015 being over $1,000,000,000 and the wealth reports which identified Customer 29 to be a foreign PEP.

On various occasions between 9 January 2018 and 19 September 2019, Crown Melbourne rated Customer 29's risk as high.

See paragraph 481.

1395. It was not until February 2019 that Customer 29 was rated high risk by Crown Perth.

Particulars

On 9 July 2012, Crown Perth rated Customer 29's risk as moderate.

On 7 April 2019, Crown Perth rated Customer 29's risk as low.

In was not until 8 February 2019 that Crown Perth reviewed Customer 29's ML/TF risk level at a compliance officer meeting and rated Customer 29's risk as high.

This is despite the significant junket turnover Customer 29 recorded at Crown Perth by 1 March 2016 and the two different passports presented by Customer 29 at Crown Perth.

1396. On and from 1 March 2016 designated services provided to Customer 29 posed higher ML/TF risks including because the provision of designated services to Customer 29 involved a combination of the following factors:

a. Customer 29 was a foreign PEP: see paragraphs 118 and 663;

b. Customer 29 was a junket player;

c. Customer 29 received high value financial (table 1, s6) and gaming services (table 3, s6) provided through multiple junket programs, including large credit facilities: see paragraph 473ff;

d. Customer 29 was a key player on the Suncity and Meg-Star junkets, as well as playing on other junkets;

e. by 2018, Crown Melbourne recorded Customer 29's total junket activity as exceeding a cumulative turnover of $6,122,000,000 with a cumulative loss of $14,777,770;

f. between 14 October 2016 and 6 August 2017, Crown Perth recorded that a junket under which Customer 29 was the primary or sole key player recorded a turnover of $310,000,000;

g. designated services provided to Customer 29 lacked transparency as the services were provided through the channel of junket programs: see paragraph 477(e). Customer 29 was the primary or sole key player in most junkets that he participated in;

h. designated services provided to Customer 29 involved large transfers to and from third parties, including to junket operators, third parties and foreign remittance services: see paragraph 456ff;

i. Customer 29 received a large transfer from another Australian casino: see paragraphs 398ff and 407ff;

j. designated services provided to Customer 29 involved large cross-border movements of funds: see paragraph 238(d);

k. at various times, Customer 29 had significant parked or dormant funds in his DAB accounts: see paragraph 252;

l. Customer 29 engaged in other transactions indicative of ML/TF typologies and vulnerabilities, including international transfers by third parties and transfers by overseas money remitters: see paragraph 24;

m. large values were transferred to and from Customer 29's bank accounts and his DAB account, and to and from other customers' DAB accounts, involving the provision by Crown Melbourne of designated services within the meaning of items 31 and 32, table 1, s6 of the Act: see paragraphs 411ff and 492;

n. at various times, Customer 29 was provided with significant amounts of credit upon request, up to limits of $5,000,000 and an additional line of credit for one trip only of $13,000,000: see paragraph 280ff;

o. Customer 29 would use his significant credit to draw down funds and transfer them to a junket operator for his use during junket programs in which he was the sole key player. Customer 29's reason for this suspicious activity was that he preferred to be discreet in respect of his gaming activity. Customer 29's cumulative junket turnover exceeded $6,400,000,000;

p. on multiple occasions, Crown Melbourne made available the Crown private jet for Customer 40. There were inadequate controls on the carrying of large amounts of cash on Crown's private jets: see paragraphs 454 and 491(c);

q. these transactions took place against the background of:

    i. law enforcement having expressed an interest in Customer 29 in 2012;

    ii. by 1 March 2016, Customer 29 engaged in transactions indicative of ML/TF typologies and vulnerabilities, including international transfers by third parties and transfers by overseas money remitters: see paragraph 24;

iii. 17 SMRs being given to the AUSTRAC CEO by Crown Melbourne and three SMRs being given by Crown Perth by 1 March 2016;

r. Customer 29 was the subject of multiple law enforcement inquiries in 2018;

s. by 1 March 2016, Crown Melbourne and Crown Perth were aware that Customer 29 travelled using several identifying documents which used different names and had different dates of birth;

t. by September 2019, Crown Melbourne was aware of ongoing Federal Court proceedings brought by the Deputy Commissioner of Taxation against Customer 29; and

u. by reason of the matters set out at subparagraphs a. to t. above, there were real risks that Customer 29's source of wealth and source of funds were not legitimate.

Monitoring of Customer 29's transactions

1397. At no time did Crown Melbourne and Crown Perth appropriately monitor Customer 29's transactions on a risk-basis.

Particulars

Section 36(1)(a), (b) of the Act and rules 15.4 to 15.8 of the Rules.

Crown Melbourne and Crown Perth were unable to monitor the ML/TF risks posed by Customer 29's transactions appropriately because they did not make and keep appropriate records of designated services provided to junket players: see paragraphs 483ff.

Crown Melbourne and Crown Perth did not apply appropriate risk-based transaction monitoring to designated services provided to Customer 29: see paragraphs 590ff, 629 to 642 and 643 to 649.

Customer 29 should have been identified to be a foreign PEP at all times on and from 1 March 2016 and his transactions monitored: r15.11.

Customer 29's transactions involved repeated transactions indicative of ML/TF typologies and vulnerabilities that were not detected prior to a 2020 lookback. Had appropriate risk-based transaction monitoring been applied, these transactions could have been identified earlier: see paragraphs 686 and 687.

In 2021, an independent auditor identified Customer 29 as responsive to an ML/TF 'risk area' as a result of Customer 29's activity as a junket player. The independent auditor noted that junkets are high risk for casino ML/TF activity and therefore patrons identified as junket players who fit certain criteria, including Customer 29, presented a higher ML/TF risk to Crown Melbourne and Crown Perth.

Transactions indicative of ML/TF typologies – third party transfers

Customer 29 was involved a number of transactions that were identified by an independent auditor in 2020 as indicative of ML/TF typologies, including international third party transfers and transfers from a foreign third party remitter:

- on 17 October 2016, Customer 29 received two telegraphic transfers of $100,000 from a company account and $1,351,300 from a second company account: SMR dated 18 October 2016; and
- on 24 January 2017, Customer 29 received a telegraphic transfer of $1,869,260 from a company account and $827,000 from a second company account, Company 13.

Inadequate controls on Crown's private jets

Between 17 May 2016 and 30 July 2016, Crown Melbourne provided Customer 29 with access to a Crown private jet on seven occasions. The number of passengers on each flight ranged from nine to 13 people. Five of the occasions were domestic Australian flights. In addition, Customer 29 was provided access to a Crown private jet to fly between foreign countries and from a foreign country to Perth.

There were inadequate controls on the carrying of large amounts of cash on Crown's private jets: see paragraphs 454 and 491(c).

1398. In 2016, despite the high ML/TF risks posed by the provision of designated services to Customer 29 pleaded in paragraphs 1390, 1396, 1397, and 1400, Crown Melbourne actively sought to develop its business relationship with Customer 29.

Particulars

In April 2016, a meeting took place at Customer 29's home between himself and several Crown Melbourne staff members. At the meeting, Customer 29 was presented with a limited-edition luxury pen and a birthday cake. Customer 29 provided feedback to the Crown Melbourne staff members that gaming activities were not up to the standard at other Australian casinos and offered recommendations to improve.

In July 2016 a Crown Melbourne staff member discussed with Customer 29 his recent trip to Crown Aspinalls. The staff member said that they had promoted Crown Perth to Customer 29. The comment recorded that Customer 29 enjoyed Crown's private jet. Crown Melbourne staff had offered to host Customer 29's granddaughter's 100-day party at Crown Melbourne.

Ongoing customer due diligence

1399. On and from 1 March 2016, on multiple occasions, the provision of designated services to Customer 29 raised red flags reflective of higher ML/TF risks as a result of Customer 29's frequent, large transactions with a number of third parties including company accounts and an Australian casino.

Particulars

See paragraphs 420ff and 456ff.

Third party transactions in 2017

In January 2017, Customer 29 received telegraphic transfers totalling $1,879,700 from a company account and $800,000 from Company 13's account.

On 11 May 2017, a junket operator under which Customer 29 was a key player, Person 44, transferred $5,000,000 to Customer 29's Australian company, Company 15.

On 13 October 2017, Customer 29 received telegraphic transfers totalling $6,772,068 from a company account.

On 10 November 2017, Customer 29 received telegraphic transfers $1,009,726.95 from a company account. Crown Melbourne conducted company searches before accepting the funds.

In October and November 2017, Customer 29 received at least $5,184,438 from a company account. A letter was sent to the company's director for signature in respect to at least part of the funds before they were accepted.

Third party transactions in 2018

On 2 August 2018, Customer 29 received a telegraphic transfer of AU$709,986 in a foreign currency from Crown Aspinalls into his Crown Melbourne DAB account.

In September 2018, Customer 29 received a telegraphic transfer of $3,773,136 from Company 13 and $1,957,177 from a second company.

In October 2018, Customer 29 received a telegraphic transfer of $1,892,317 from an Australian casino and $78,000 from Company 13's account.

In December 2018, Customer 29 travelled overseas and was unable to return due to the cancellation of his visa.

1400. On and from 1 March 2016, on multiple occasions, the provision of designated services to Customer 29 raised red flags reflective of higher ML/TF risks as a result of complex, unusual large transactions and unusual patterns of transactions involving Customer 29 which had no apparent economic or visible lawful purpose.

Particulars

See paragraph 477.

Unusual transactions and patterns of transactions in 2016

On 14 October 2016, Customer 29 transferred $3,492,541 from his personal account to his Crown Melbourne DAB account.

On 22 November 2016, Customer 29 had a CCF of $5,000,000 and a TTO of $10,000,000 approved for a trip commencing the following day.

Unusual transactions and patterns of transactions in 2017

In January 2017, Customer 29 had made a debt repayment to Crown Melbourne of $5,600,000.

By February 2017, Customer 29 had a cumulative individual and junket turnover at Crown Melbourne and Crown Perth of $1,500,000,000.

On 25 February 2017, Customer 29 transferred from his Crown Melbourne DAB account to his personal account a total of $11,592,745.

On 21 July 2017, Customer 29 had a debt to Crown Melbourne of $8,154,860. On 11 August 2017, Customer 29 transferred $8,438,160 from his personal account into his Crown Melbourne DAB account for the repayment of his debt. On 6 September 2017, Customer 29 transferred $8,438,160 from his Crown Melbourne DAB account to his personal account.

By 14 September 2017, a junket of a junket operator, Person 44, whose sole or primary customer appeared to be Customer 29 was noted as not having a CCF as funds were transferred directly from Customer 29 for use. The junket had a cumulative Crown Melbourne turnover of $2,498,000,000 (nearly half of which had occurred in the previous year) with a cumulative loss of $25,100,000. Between 14 October 2016 and 6 August 2017, the junket had a cumulative Crown Perth turnover of $310,000,000 with a cumulative loss of $2,000,000.

The junket operator, Person 44, was a former Crown sales staff member who Crown had assigned to facilitate Customer 29's gambling and travel to Crown. Customer 29 later appointed Person 44 to prominent roles, including being his personal adviser.

By 14 September 2017, an application to become a junket operator made by Person 42, a person whose sole or primary customer appeared to be Customer 29, was recommended to be allowed to commence business. Customer 29 who was the junket operator's sole player in other Sydney and Gold Coast casinos. The junket operator was noted as not having a CCF as funds were transferred directly from Customer 29 for use. The Senior Vice President (International Business) identified that Customer 29 preferred to be discreet which explained his desire to play under a junket program rather than on an individual premium program. On 20 September 2017, the junket operator was approved as a junket operator at Crown Melbourne.

On 15 September 2017, Customer 29 was approved for $5,000,000 with a TTO of $10,000,000.

On 25 October 2017, Customer 29 transferred $6,447,440 from his personal account to his Crown Melbourne DAB account.

On 26 October 2017, Customer 29 transferred $6,447,495 to a junket operator, Person 44.

On 28 November 2017, Customer 29's TTO was raised to $8,000,000 (with an additional basic line of $5,000,000).

Between 28 November 2017 and 28 December 2017, Customer 29 attended a junket program of Person 44 as the only junket player.

In 2017, a junket operator, Person 44, transferred to Customer 29 a total of $9,405,438.

Unusual transactions and patterns of transactions in 2018

On 9 January 2018, Crown Melbourne and Crown Perth first determined Customer 29 to be a foreign PEP. This was despite the two 2015 wealth reports which identified Customer 29 to be a foreign PEP: paragraph 1391.

By 10 January 2018, Customer 29 had a CCF limit of $5,000,000, a CCF balance of $13,000,000, a safekeeping balance of $110,240, a non-gaming balance of $11,915 and a table balance of $50,000.

On 27 June 2018, while playing on a junket program, Customer 29 played baccarat with a turnover in the tens of millions of dollars and an average bet of approximately $300,000.

By 4 September 2018, Customer 29 had a CCF limit of $5,000,000 and a CCF balance of $8,389,640. By 5 September 2018, Customer 29 had an outstanding debt to Crown Melbourne of $8,389,664.

Between 1 September 2018 and 31 September 2018, Customer 29 was a key player on a Suncity junket program. Customer 29 had a turnover of $690,400 with a win of $40,500.

By 1 October 2018, Customer 29 had an outstanding debt to Crown Melbourne of $2,659,351.10. By 2 October 2018, that outstanding debt had been reduced to $757,000 and a CCF appears to have been approved of $13,000,000.

On 12 October 2018, Customer 29 transferred $12,000,000 to a junket operator, Person 42.

On 14 October 2018, Customer 29 received a transfer of $12,000,000 from a junket operator, Person 42.

On 30 October 2018, Customer 29 received a telegraphic transfer into his personal account of $16,296,280 from a junket operator, Person 42.

Between 1 October 2018 and 31 October 2018, Customer 29 was a key player on a Suncity junket program. Customer 29 had a turnover of $212,325 with a loss of $50,000.

On 21 November 2018, Crown Melbourne approved a TTO of $13,000,000 in addition to Customer 29's CCF of $5,000,000 for a trip commencing on 22 November 2018.

By 17 December 2018, a junket operator, Person 44, whose sole or primary customer appeared to be Customer 29 had a cumulative

Crown Melbourne turnover of $3,544,000,000 with a cumulative loss of $370,000. The junket had a cumulative Crown Perth turnover of $310,000,000 with a cumulative loss of $2,800,000.

Between 1 December 2018 and 31 December 2018, Customer 29 was a key player on a Meg-Star junket program. Customer 29 had a turnover $427,600 with a loss of $42,680.

Unusual transactions and patterns of transactions in 2019

On 21 May 2019, Customer 29 transferred $2,477,523 to a junket operator, Person 42.

By 2 August 2019, the two junket operators, Person 42 and Person 44, under which Customer 29 was the primary or only key player had a cumulative Crown Melbourne turnover of $3,558,000,000 and $1,897,000,000 respectively with a cumulative loss of $100,000 and $21,000,000 respectively. One of the junket operators was known to be the marketing manager of Customer 29's Australian company, Company 15, and the daughter of the other junket operator.

In December 2018, Customer 29 travelled overseas and was unable to return due to the cancellation of his visa.

On 20 January 2021, Customer 29 was issued a WOL at Crown Melbourne as a result of the application of the SPR process: see particulars to paragraph 1234.

As at 11 February 2021, no NRL has been issued in respect of Customer 29 at Crown Perth.

1401. On and from 1 March 2016, on multiple occasions, the provision of designated services to Customer 29 raised red flags reflective of higher ML/TF risks as a result of receiving numerous inquiries from law enforcement agencies in respect of Customer 29.

Particulars

In February 2018, Crown Melbourne received a law enforcement inquiry in respect of Customer 29.

In May 2018, Crown Melbourne received a law enforcement inquiry in respect of Customer 29. The inquiry related to junket operations and taxation.

1402. On and from 19 September 2019, Crown Melbourne was aware of court proceedings identifying Customer 29 in connection with a taxation penalty.

Particulars

On 19 September 2019, Crown senior management circulated a Federal Court of Australia decision in which Customer 29 was the respondent. Crown Senior Legal Counsel noted that Customer 29 had his visa cancelled and so was unable to return to Australia, and suggested that Crown Melbourne ban Customer 29 given the sensitivities surrounding Customer 29. Customer 29 was not issued with a WOL at Crown Melbourne until January 2021 and was never issued with an NRL at Crown Perth.

The Federal Court decision relevantly found that:

- AUSTRAC records showed tens of millions of dollars transferred into and out of Australia between January 2016 and August 2019. Between December 2018 and August 2019, the amount transferred out of Australia exceeded the amount transferred in by over $45,000,000, nearly double the year before,
- Customer 29 had significant business interests in foreign countries and the structures and operations of his foreign companies allow Customer 29 easily to move assets between jurisdictions.

1403. At no time did Crown Melbourne or Crown Perth undertake appropriate risk-based customer due diligence with respect to Customer 29 with a view to identifying, mitigating and managing the ML/TF risks posed by the provision of designated services on and from 1 March 2016.

a. Crown Melbourne and Crown Perth took steps to understand Customer 29's source of wealth/funds. However, neither Crown Melbourne nor Crown Perth took appropriate steps to determine whether that source was legitimate.

b. At no time did Crown Melbourne or Crown Perth take appropriate steps to identify or analyse the ML/TF risks of Customer 29's transactions or to consider whether they had a lawful purpose.

c. Other that in October and November 2017, Crown Melbourne and Crown Perth gave no consideration at any time to whether large and high risk transactions should be processed. In October and November 2017, Crown Melbourne conducted company searches and required the directors of a third party company to provide a signed letter prior to accepting funds from the third party company.

d. On each occasion prior to January 2021 that senior management considered whether to continue the business relationship with Customer 29, senior management failed to give adequate consideration to whether the ML/TF risks posed by Customer 29 were within Crown Melbourne's risk appetite

e. On each occasion that senior management considered whether to continue the business relationship with Customer 29, senior management failed to give adequate consideration to whether the ML/TF risks posed by Customer 29 were within Crown Perth's risk appetite.

Particulars

Section 36(1)(a) of the Act.

The due diligence steps taken with respect to Customer 29 included:

Wealth and risk intelligence reports

In July 2016, December 2016, January 2017 and June 2018, Crown Melbourne obtained wealth reports in respect of Customer 29 which set out his substantial personal wealth, history of political donations and known associates. The December 2016 report included that Customer 29 had been caught up in a far-reaching corruption scandal involving senior government officials in his home country which had prompted his departure.

In December 2016, Crown Melbourne obtained a risk intelligence report in respect of Customer 29, based on his two different names and birthdates on identifying documents. The report noted Customer 29's estimated net worth, his status as a foreign PEP and his business interests.

Database searches

Between July 2016 and August 2019, Crown Melbourne and Crown Perth conducted risk intelligence, company, land registry and property searches in respect of Customer 29.

At no point, as a result of these searches, did Crown Perth appropriately consider the ML/TF risks of the source of Customer 29's wealth/funds or whether an ongoing business relationship with Customer 29 was within its ML/TF risk appetite.

Junket and credit profiles

Crown Melbourne's credit team considered Customer 29's creditworthiness in November 2016 and conducted a number of due diligences searches for that purpose.

On 14 September 2017, junket profiles for two separate junket operators, Person 42 and Person 44. Each profile noted that Customer 29 appeared to be the junket operator's sole or primary customer.

The Senior Vice President (International Business) identified that Customer 29 preferred to be discreet which explained his desire to play under a junket program rather than on an individual premium program.

Transactions monitoring

In October and November 2017, Customer 29 received telegraphic transfers from company accounts: paragraph 0. Crown Melbourne conducted company searches and a letter was sent to the companies' director for signature in respect to at least part of the funds before they were accepted.

In September 2018, new guidelines regarding receiving funds from companies meant that Crown Melbourne identified several companies that had previously sent funds to Customer 29 could no longer do so.

Customer 29 departed from Australia in December 2018 and has not been able to return since.

Other due diligence conducted

In August 2019, Crown Melbourne conducted a targeted media report search in respect of Customer 29 and any mentions of an organised crime syndicate or 'Laundering'. The AML Manager emailed the Chief Legal Officer (Australian Resorts) copies of the results along with Customer 29's wealth reports.

Senior management engagement

From November 2016, Crown Melbourne held a number of VIP Operations meetings which concerned Customer 29 that were attended by senior management:

- in November 2016, the attendees considered whether to continue a business relationship with Customer 29. This decision was not based on ML risks but rather reputational risks associated with doing business with citizens from a particular foreign country. Customer 29 had evidence of citizenship from another foreign country and was therefore approved for business. The minutes recorded that Customer 29 had been encouraged to play on an individual premium program at 80% and had requested a personal invitation to Crown Towers Perth. In December 2016, a meeting with the Chief Executive Officer of Crown Resorts Ltd, a Crown Resorts director, the Executive General Manager (Legal and Regulatory Services), Chief Executive officer (Australian Resorts), the Senior Vice President (International Business) and the General Manager (VIP International) confirmed the decision to continue doing business with Customer 29;
- in December 2016, the attendees considered a wealth report that stated that Customer 29 was a close associate of two government officials in a foreign country who were arrested for corruption, but that Customer 29 was considered by the Committee to be welcome to visit in any case; and
- in January 2017, the minutes recorded that Customer 29 had paid a debt to Crown Melbourne of $5,600,000.

In February 2017, a Group Credit Manager (VIP International) conducted due diligence in respect of Customer 29. The Group Credit Manager recommended that Customer 29 play under a junket operator, Person 44.

In January 2018, the CTRM forwarded to the Group General Manager (AML) several articles relating to Customer 29, noting that Customer 29 was a foreign PEP and alerts had been placed on his profile. The CTRM asked the Group General Manager (AML) for approval to continue a business relationship with, and provide designated services to, Customer 29.

The Group General Manager (AML) asked that the matter be discussed further. The Group General Manager (AML) determined that continuing a business relationship with Customer 29 was within Crown's ML/TF risk appetite, despite his status as a foreign PEP as pleaded at paragraph 1391 and the matters pleaded at paragraphs 1390, 1396, 1397, 0, 1400, 1401 and 1402, on the condition that his risk rating was updated and his transactions were monitored.

In May 2018, the Group General Manager (AML) collected due diligence on Customer 29 as part of a due diligence exercise

conducted in respect of key players on the Suncity junket program. She notified the Chief Legal Officer (Australian Resorts) that she was additionally conducting ECDD.

By no later than June 2018, the Chief Legal Officer (Australian Resorts), who was also the AML Compliance Officer at both Crown Melbourne and Crown Perth, was briefed by the Group General Manager (AML) on AML concerns in respect of repayment of debt from offshore. The brief referred to a $12,700,000 debt repaid by Customer 29 to Crown through multiple third party accounts and that Crown had been unable to connect any of those accounts to Customer 29. The brief identified that Customer 29 was well known to Crown.

In July 2019, the Group General Manager (AML) requested documentation held by Crown in respect of Customer 29.

In July 2019, in response to a media segment which named Customer 29, Crown's Senior Legal Counsel emailed Customer 29's patron information to the Chief Legal Officer (Australian Resorts). Adverse entries noted for Customer 29 were his associations with adverse government officials in a foreign country. Crown Melbourne conducted a media report search in respect of Customer 29 which returned more than 1,800 articles, 40 of which were extracted and sent by the Group General Manager (AML) to the Chief Legal Officer (Australian Resorts). A risk intelligence and company search were conducted in respect of Customer 29 and his due diligence documents were compiled. No further action was taken.

On 20 January 2021, POI Group Committee meeting considered Customer 29 and determined to issue him with a WOL and an NRL as a result of the ILGA matter.

On 20 January 2021, Crown Melbourne issued Customer 29 with a WOL.

There is no record of Crown Perth issuing Customer 29 with an NRL.

On 24 March 2021, the AML Manager requested that Crown Perth provide CURA and financial transaction reports for Customer 29. The Legal Officer (AML) who provided the documents noted that two CURA reports existed for Customer 29, that he appeared to be known by two different names, and that she was not sure why that was the case.

None of these steps were proportionate to the ML/TF risks reasonably posed by Customer 29 on and from 1 March 2016.

Enhanced customer due diligence

1404. Having formed a suspicion for the purposes of s41 of the Act, Crown Melbourne gave the AUSTRAC CEO SMRs with respect to Customer 29 on:

a. 18 October 2016;

b. 16 October 2017; and

c. 5 January 2018.

Particulars

The 18 October 2016 SMR identified two telegraphic transfers received by Customer 29 from company accounts totalling $1,451,300. The grounds of suspicion were based on Customer 29's annual losses, the amount of cash Customer 29 was prepared to carry and the third party transactions.

The 16 October 2017 SMR identified 19 telegraphic transfers received for Customer 29 totalling several million dollars from third party company accounts.

The 5 January 2018 SMR identified that Customer 29's passports had two different names and birthdates and that Customer 29 was prepared to carry significant amounts of cash.

1405. On each occasion that Crown Melbourne formed a suspicion with respect to Customer 29 for the purposes of s41 of the Act, it was required to apply its ECDD program to Customer 29.

Particulars

Rule 15.9(3) of the Rules.

1406. Crown Melbourne did not carry out appropriate risk-based ECDD measures with respect to Customer 29 on each occasion that Crown Melbourne formed a suspicion with respect to Customer 29 for the purposes of s41 of the Act.

a. There are no records of ECDD being conducted following the lodgement of SMR on 18 October 2016 or 16 October 2017: see paragraphs 664 and 685.

b. Crown Melbourne and Crown Perth did not assess Customer 29's source of wealth/funds with respect to the designated services it was providing to him from a ML/TF perspective.

c. Appropriate risk-based steps were not taken to analyse and monitor Customer 29's transactions – both past and future – including to understand their economic purpose: see paragraph 590 and 666.

d. On each occasion prior to January 2021 that senior management considered whether to continue the business relationship with Customer 29, senior management failed to give adequate consideration to whether the ML/TF risks posed by Customer 29 were within Crown Melbourne's risk appetite.

Particulars

Rules 15.9(3), 15.10(1)(c), (d), (2), (5) and (6) of the Rules.

The only ECDD conducted following the lodgement of the SMR on 5 January 2018 was an open source media search in respect of Customer 29. There was no attempt to carry out a ML/TF risk-based assessment in respect of Customer 29: Rule 15.9(3) of the Rules.

In January 2018, the Group General Manager (AML) determined that continuing a business relationship with Customer 29 was within Crown's ML/TF risk appetite, despite his status as a foreign PEP

pleaded at paragraph 1391 and the matters pleaded at paragraphs 1390, 1396, 1397, 0, 1400, 1401 and 1402, on the condition that his risk rating was updated and his transactions were monitored. However, Crown did not apply appropriate risk-based transaction monitoring to designated services provided to Customer 29.

After 10 January 2018, Crown Melbourne allowed Customer 29 to make regular and significant transactions despite the high ML/TF risks as pleaded at paragraphs 1390, 1396, 1397, 0, 1400, 1401 and 1402.

1407. At all times from 1 March 2016, Customer 29 was a foreign PEP.

Particulars

See particulars to paragraph 1391.

1408. At all times from 1 March 2016, Crown Melbourne and Crown Perth were required to apply its ECDD program to Customer 29.

Particulars

Rules 15.9(2), 15.11 of the Rules

See paragraphs 660, 663 and 666.

1409. Crown Melbourne and Crown Perth did not carry out appropriate risk-based ECDD measures with respect to Customer 29 on and from 1 March 2016 given his status as a foreign PEP. In particular:

a. Crown Melbourne did not undertake a detailed analysis of Customer 29's KYC information or analyse the legitimacy of Customer 29's source of wealth/funds;

b. on occasions where senior management approved a continuing business relationship with Customer 29 as a foreign PEP, the decision did not have adequate regard to the ML/TF risks posed by Customer 29 given his status as a foreign PEP. Further, the approval was conditional on transaction monitoring being adequately and appropriately applied in respect of Customer 29, and this condition was not met; and

c. on occasions where senior management approved continuing to provide designated services to Customer 29 as a foreign PEP, the decision did not have adequate regard to the ML/TF risks posed by Customer 29 given his status as a foreign PEP. Further, approval was conditional on transaction monitoring being adequately and appropriately applied in respect of Customer 29, and this condition was not met.

Particulars

Rules 15.10(2), 15.10(6), 15.11 of the Rules.

See particulars to paragraphs 1403 and 1406.

See paragraph 660, 663, 666, 667 and 668.

1410. On and from 9 January 2018, Crown Melbourne rated Customer 29 high risk.

Particulars

Crown Melbourne rated Customer 29 high risk on eight occasions between 9 January 2018 and 19 September 2019: paragraph 1394

1411. On 8 February 2019, Crown Perth rated Customer 29 high risk.

Particulars

Crown Perth rated Customer 29 high risk on 8 February 2019: see paragraph 1395.

1412. On each occasion that Crown Melbourne or Crown Perth rated Customer 29 high risk, Crown Melbourne or Crown Perth was required to apply its ECDD program to Customer 29.

Particulars

Rule 15.9(1).

1413. Crown Melbourne and Crown Perth did not carry out appropriate risk-based ECDD measures with respect to Customer 29 on each occasion that Crown Melbourne or Crown Perth rated Customer 29 high risk.

Particulars

See particulars to paragraphs 1403 and 1406.

1414. By reason of the matters pleaded from paragraphs 1384 to 1413, on and from 1 March 2016, Crown Melbourne and Crown Perth:

a. did not monitor Customer 29 in relation to the provision of designated services, with a view to identifying, mitigating and managing the ML/TF risks it reasonably faced; and

b. did not do so in accordance with rr 15.5 and 15.9 of the Rules.

1415. By reason of the matters pleaded at paragraph 1414, Crown Melbourne contravened s36(1) of the Act on and from 1 March 2016 to January 2021 with respect to Customer 29.

1416. By reason of the matters pleaded at paragraph 1414, Crown Perth contravened s36(1) of the Act on and from 1 March 2016 with respect to Customer 29.

Particulars

Section 36(1) of the Act is a civil penalty provision: s36(2) of the Act.

Customer 30

1417. Customer 30 was a customer of Crown Melbourne from 31 August 2009 to 16 December 2020.

1418. From at least 31 August 2009 to 16 December 2020, Crown Melbourne provided Customer 30 with designated services within the meaning of table 1 and table 3, s6 of the Act.

Particulars

On 31 August 2009, Crown Melbourne opened a DAB account and safekeeping account (AUD) for Customer 30, which remain open.

From 14 January 2010 to 2 September 2015, Customer 30 was subject to a WOL.

Crown Melbourne recorded Customer 30's rated gaming activity between 2009 to 14 September 2016 as a cumulative loss of $1,881,670.

The ML/TF risks posed by Customer 30

1419. At all times from 1 March 2016, Crown Melbourne rated Customer 30 as high risk.

Particulars

On various occasions between September 2009 and March 2018, Crown Melbourne assessed Customer 30 as high risk.

1420. By 16 December 2009, Crown Melbourne was on notice that funds used by Customer 30 at Crown Melbourne originated from a fraudulent cheque.

Particulars

In December 2009, Crown Melbourne was contacted by an Australian bank who indicated that $480,000 of an altered company cheque made out for $507,000 had been transferred to Customer 30's bank account at another financial institution and then deposited into Customer 30's Crown Melbourne DAB account.

1421. By 14 January 2010, Crown Melbourne was on notice that Customer 30 was a person of interest in respect of money laundering charges at Crown Melbourne casino.

Particulars

By early 2010, Crown Melbourne was aware of a media article which identified that a person with Customer 30's name, age and nationality had been arrested in late 2009 and charged with multiple counts of laundering in the sum of over $500,000 at Crown Melbourne. The article reported police allegations that the individual had cashed a stolen cheque, mixed the funds with another $480,000 bank transfer and $500,000 in cash before playing at Crown Melbourne and leaving with more than $1,000,000 in cash and casino chips.

On 14 January 2010, Crown Melbourne issued a WOL in respect of Customer 30.

On 14 September 2010, a Crown employee entered a comment on a Crown Melbourne customer management system which said that during the Court proceedings Customer 30 stated that he engaged in lending money to people at Crown Casino.

1422. On 2 September 2015, Crown Melbourne revoked the WOL issued in respect of Customer 30 despite being on notice that he had been charged with money laundering offences while on Crown Melbourne's premises.

Particulars

In August 2013, Crown Melbourne was informed that Customer 30 was acquitted of the money laundering charges in 2011 and Customer 30 requested the revocation of the WOL issued in respect of him.

On 6 September 2013, Crown Melbourne refused to revoke the WOL issued in respect of Customer 30.

In June 2015, Customer 30 made a further request to Crown Melbourne for the revocation of the WOL issued in respect of him. Customer 30 identified that he had been acquitted of the money laundering charges, had no other criminal record, would obey Crown Melbourne's rules and would introduce Crown Melbourne to his foreign business circle friends. The letter attached a National Police Certificate which did not return any disclosable court outcomes.

On 1 September 2015, a Manager (Compliance Reporting) reviewed comments about Customer 30 in SEER which noted that Customer 30 has stated during Court proceedings that he 'lends money to people at the Casino'. The manager expressed the view that, based on that information, he was minded not to revoke Customer 30's WOL.

On 2 September 2015, the Crown Melbourne POI Committee decided to revoke the WOL issued in respect of Customer 30.

1423. By 1 March 2016, higher ML/TF risks were indicated by the nature and purpose of Customer 30's business relationship with Crown Melbourne, the nature of the transactions he had been conducting, together with the suspicions Crown Melbourne itself had formed with respect to Customer 30.

Particulars

Section 36(1)(a), (b) of the Act and Chapter 15 of the Rules.

By the matters in paragraphs 1421 and 1422, Crown Melbourne was aware that Customer 30 had been the subject of money laundering charges related to designated services provided at Crown Melbourne. Crown Melbourne was also aware that Customer 30 had stated that he engaged in lending money to persons at Crown casino.

SMRs by 1 March 2016

By 1 March 2016, Crown Melbourne had given the AUSTRAC CEO 15 SMRs in relation to Customer 30 – on 2 September 2009, 4 September 2009, 7 September 2009, 9 September 2009, 14 September 2009, 16 September 2009, 14 October 2009, 16 December 2009, 17 December 2009, 18 December 2009, 5 May 2010, 16 November 2015, 18 November 2015, 24 November 2015 and 30 November 2015.

Each SMR reported similar repeated patterns of suspicions relating to annual losses, annual bets, third party transactions, low gaming activity given high value of transactions, suspicious cash transactions and the amount of cash Customer 30 was prepared to carry.

Large and suspicious transactions by 1 March 2016

On 6 September 2009, Customer 30 requested an exchange of $406,600 of gaming chips to cash. Customer 30 was asked if he would prefer a telegraphic transfer or cheque for security reasons. He

refused, stating that he wanted cash, was comfortable carrying large amounts of cash and carried large amounts of cash when travelling to Melbourne.

Between 11 November 2015 and 30 November 2015, shortly after the first WOL was lifted, designated services provided to Customer 30 involved repeated large cash transactions. The transactions totalled, at least, account deposits of $1,386,400, chip cash-ins of $554,720 and a buy-in of $20,000.

By 30 November 2015, two months after the first WOL was lifted, Crown Melbourne recorded that Customer 30 had total losses of $1,119,765 and an increase in average bet from $9,570 in 2009 to $13,030 in 2015.

In 2015 and 2016, Customer 30 engaged in transactions indicative of ML/TF typologies involving the use of third party agents:

- on 27 November 2015, Crown Melbourne was credited $50,000 by an EFT transaction for further credit of Customer 30 with transaction narrative such that it was not able to be determined whether the third party was a patron or a non-patron;
- on 10 December 2015, Crown Melbourne was credited $100,000 by an EFT transaction for further credit of Customer 30 with transaction narrative such that it was not able to be determine whether the third party was a patron or a non-patron; and
- on 6 January 2016, Crown Melbourne was credited $50,000 by an EFT transaction for further credit of Customer 30 with transaction narrative such that it was not able to be determined whether the third party was a patron or a non-patron.

By 1 March 2016, the SMRs identified cash deposits that totalled $1,640,000, cash withdrawals that totalled $620,781 and exchanges of gaming chips to cash that totalled $491,970.

Law enforcement inquiries by 1 March 2016

On 13 August 2014 and 10 September 2014, Customer 30 was the subject of a law enforcement inquiry.

On 3 February 2016, Customer 30 was the subject of a law enforcement inquiry.

1424. At all times on and from 1 March 2016, Customer 30 was recognised by Crown Melbourne to be a high risk customer.

Particulars

On various occasions between 17 December 2009 and 9 March 2018, Crown Melbourne assessed Customer 30 as high risk.

See paragraph 120.

1425. On and from 1 March 2016 designated services provided to Customer 30 posed higher ML/TF risks including because the provision of designated services to Customer 30 involved a combination of the following factors:

a. Customer 30 received high value financial (table 1, s6) and gaming services (table 3, s6);

b. by no later than 14 September 2016, Crown Melbourne recorded Customer 30's individual rated gaming activity as a cumulative loss of $1,881,670;

c. Crown Melbourne made available the Crown private jet for Customer 30. There were inadequate controls on the carrying of large amounts of cash on Crown's private jets: see paragraphs 454 and 491(c);

d. these transactions took place against the background of:

i. law enforcement having expressed an interest in Customer 30 in 2014 and shortly before 1 March 2016, on 3 February 2016;

ii. designated services provided to Customer 30 involved repeated large cash transactions;

iii. Customer 30 engaged in transactions indicative of ML/TF typologies involving use of third party agents;

iv. 15 SMRs being given to the AUSTRAC CEO by Crown Melbourne by 1 March 2016;

e. by 14 January 2010, Crown Melbourne was on notice that Customer 30 was a person of interest in respect of money laundering charges at Crown Melbourne casino;

f. by February 2017, Crown Melbourne was on notice that a law enforcement agency had considered it necessary in the public interest to prohibit Customer 30 from entering or remaining in a casino or a casino complex; and

g. by reason of the matters set out at subparagraphs a. to f. above, there were real risks that Customer 30's source of wealth and source of funds were not legitimate.

Monitoring of Customer 30's transactions

1426. At no time on and from 1 March 2016 did Crown Melbourne appropriately monitor Customer 30's transactions on a risk-basis.

Particulars

Section 36(1)(a), (b) of the Act and rules 15.4 to 15.8 of the Rules.

Crown Melbourne did not apply appropriate risk-based transaction monitoring to designated services provided to Customer 30: see paragraphs 629 to 642 (designated services).

Inadequate controls on Crown's private jets

On 16 July 2016 and 18 July 2016, Crown Melbourne provided Customer 30 with access to a Crown private jet from the Gold Coast to Melbourne and from Melbourne an overseas country for seven people.

There were inadequate controls on the carrying of large amounts of cash on Crown's private jets: see paragraphs 454 and 491(c).

Ongoing customer due diligence

1427. On and from 1 March 2016, the provision of designated services to Customer 30 by Crown Melbourne raised red flags reflective of higher ML/TF risks.

Particulars

At all times since 1 March 2016, Crown Melbourne has maintained a DAB account and safekeeping account for Customer 30.

On 3 March 2016, Customer 30's losses for the year (from January 2016) totalled $341,785.

By 14 September 2016, Customer 30's losses for the year had increased to $621,145.

1428. On and from February 2017, Crown Melbourne was aware that a law enforcement agency had considered it necessary in the public interest to prohibit Customer 30 from entering or remaining in a casino or a casino complex.

Particulars

By February 2017, Crown Melbourne applied an alert to Customer 30's patron profile indicating that Crown Melbourne had received an exclusion order from a law enforcement agency that had considered it necessary in the public interest to prohibit Customer 30 from entering or remaining in a casino or a casino complex.

Crown Melbourne did not issue Customer 30 with a WOL until 16 December 2020.

1429. At no time did Crown Melbourne undertake appropriate risk-based customer due diligence with respect to Customer 30 with a view to identifying, mitigating and managing the ML/TF risks posed by the provision of designated services on and from 1 March 2016.

a. At no time did Crown Melbourne take appropriate steps to understand whether Customer 30's source of wealth/funds was legitimate.

b. At no time did Crown Melbourne take appropriate steps to identify or analyse the ML/TF risks of Customer 30's transactions or to consider whether they had a lawful purpose.

c. After revoking Customer 30's WOL in September 2015 and until to the decision to issue Customer 30 with a WOL in December 2020, there is no record of senior management considering whether continuing the business relationship with Customer 30 was within Crown Melbourne's ML/TF risk appetite in light of the ML/TF risks posed by Customer 30.

Particulars

Section 36(1)(a) of the Act.

No due diligence steps were taken in respect of Customer 30 on and from 1 March 2016. This was not proportionate to the ML/TF risks reasonably posed by Customer 30 on and from 1 March 2016.

Enhanced customer due diligence

1430. Crown Melbourne gave the AUSTRAC CEO SMRs with respect to Customer 30 on:

a. 3 March 2016, and

b. 14 September 2016.

Particulars

Each of these SMRs reported high losses and that Customer 30 was prepared to carry large amounts of cash.

1431. On each occasion that Crown Melbourne formed a suspicion with respect to Customer 30 for the purposes of s41 of the Act, it should have conducted enhanced customer due diligence.

Particulars

Rule 15.9(3) of the Rules.

1432. Crown Melbourne did not carry out appropriate risk-based ECDD measures with respect to Customer 30 on each occasion that Crown Melbourne formed a suspicion with respect to Customer 30 for the purposes of s41 of the Act.

a. There are no records of ECDD being conducted following the lodgement of SMRs on 3 March 2016 and 14 September 2016: see paragraphs 664 and 685.

b. Appropriate risk-based steps were not taken to obtain or analyse information about Customer 30's source of wealth/funds: see paragraph 667.

c. Appropriate risk-based steps were not taken to analyse and monitor Customer 30's transactions – both past and future – including to understand their economic purpose: see paragraph 590 and 666.

d. After revoking Customer 30's WOL in September 2015 and until to the decision to issue Customer 30 with a WOL in December 2020, there is no record of senior management considering whether continuing the business relationship with Customer 30 was within Crown Melbourne's ML/TF risk appetite in light of the ML/TF risks posed by Customer 30.

Particulars

Rules 15.9(3), 15.10(1)(c), (d), (2), (5) and (6) of the Rules.

On 16 December 2020, Crown Melbourne issued Customer 30 with a WOL. This was over four years after Crown Melbourne last provided a designated service to Customer 30.

See particulars to paragraph 1429.

1433. On and from 1 March 2016, Crown Melbourne rated Customer 30 high risk.

Particulars

Crown Melbourne rated Customer 30 high risk on five occasions between 3 March 2016 and 9 March 2018: see paragraph 1419.

1434. On each occasion that Crown Melbourne rated Customer 30 high risk, Crown Melbourne was required to apply its ECDD program to Customer 30.

Particulars

Rule 15.9(1) of the Rules.

See paragraph 661.

1435. Crown Melbourne did not carry out appropriate risk-based ECDD measures with respect to Customer 30 on each occasion that Crown Melbourne rated Customer 30 high risk.

Particulars

See particulars to paragraphs 1429 and 1432.

See paragraphs 661, 666, 667 and 668.

1436. By reason of the matters pleaded from paragraphs 1417 to 1435, on and from 1 March 2016, Crown Melbourne:

a. did not monitor Customer 30 in relation to the provision of designated services, with a view to identifying, mitigating and managing the ML/TF risks it reasonably faced; and

b. did not do so in accordance with rr 15.5 and 15.9 of the Rules.

1437. By reason of the matters pleaded at paragraph 1436, Crown Melbourne contravened s36(1) of the Act on and from 1 March 2016 to December 2020 with respect to Customer 30.

Particulars

Section 36(1) of the Act is a civil penalty provision: s36(2) of the Act.

Customer 31

1438. Customer 31 has been a customer of Crown Melbourne since May 1998.

1439. From at least December 2006, Crown Melbourne provided Customer 31 with designated services within the meaning of table 1 and table 3, s6 of the Act.

Particulars

On 6 September 1998, Crown Melbourne opened a DAB account and safekeeping account for Customer 31.

On 13 May 2003, Crown Melbourne opened a credit facility for Customer 31, which was closed on 20 June 2021.

Between 1998 and 2011, Crown Melbourne recorded Customer 31's individual rated gaming activity to be a cumulative loss of $10,453,850. Customer 31's individual loss escalated from $35,700 in 1998 to $12,000,450 in 2011. Customer 31's average bet increased from $68,185 in 2006 to $276,830 in 2011.

By July 2018, Crown Melbourne recorded Customer 31's individual gaming activity as a cumulative turnover of $265,367,100 with a loss of $10,116,350.

1440. Customer 31 has been a customer of Crown Perth since June 1997.

1441. From at least December 2006, Crown Perth provided Customer 31 with designated services within the meaning of table 1 and table 3, s6 of the Act.

Particulars

On 30 April 2005, Crown Perth opened a DAB account and safekeeping account for Customer 31.

On 11 June 1996 Crown Perth opened a CCF for Customer 31, which was closed on 9 September 2005.

On 13 October 2005, Crown Perth opened a FAF account for Customer 31. On 23 November 2013, a CCF/FAF limit of $5,000,000 was approved for Customer 31. The FAF was closed on 24 June 2021.

Between 2003 and 2020, Crown Perth recorded Customer 31's individual rated gaming activity to be a cumulative loss of $27,838,262. Customer 31's individual loss escalated from $486,325 in 2003 to $9,416,000 in 2019.

The ML/TF risks posed by Customer 31

1442. By 1 March 2016, higher ML/TF risks were indicated by the nature and purpose of Customer 31's business relationship with Crown Melbourne and Crown Perth, the nature of the transactions he had been conducting, together with the suspicions Crown Melbourne and Crown Perth itself had formed with respect to Customer 31.

Particulars

Section 36(1)(a), (b) of the Act and Chapter 15 of the Rules.

SMRs by 1 March 2016

By 1 March 2016, Crown Melbourne had given the AUSTRAC CEO one SMR in relation to Customer 31 on 5 September 2011. The grounds of suspicion were based on Customer 31's annual win/losses and an increase in average bet.

By 1 March 2016, Crown Perth had given the AUSTRAC CEO one SMR in relation to Customer 31 on 26 November 2014. The grounds of suspicion were based on the third party deposit below.

Gaming activity by 1 March 2016

Crown Melbourne recorded Customer 31's individual rated gaming activity in 2011 to be a loss of $12,000,450.

Crown Perth recorded Customer 31's individual rated gaming activity to be:

- in 2011, a loss of $1,703,000;
- in 2012, a loss of $7,554,795;
- in 2013, a loss of $6,438,000;
- in 2014, a win of $585,900; and
- in 2015, a loss of $2,775,000.

Unusual transactions by 1 March 2016

Between 3 October 2014 and 14 November 2014, the Crown Perth Cage approved a release of ten sums totalling $2,416,864. The funds had been received into a Riverbank account in 34 QuickCash cash deposits made at ATMs in Perth and Sydney ranging from $15,700 to $50,000 and one telegraphic transfer of $900,000. It was not until 2021 that Crown Perth identified these transactions as indicative of the ML/TF typology of cuckoo smurfing: SMR dated 19 May 2021.

On or around 24 November 2014, Customer 31's personal assistant sent two telegraphic transfers of $800,000 and $500,000 through a money changer to his Crown Perth DAB account together with $133,200 in two QuickCash cash deposits. Twenty minutes after the funds were received, Customer 31's personal assistant requested that they be transferred to Customer 31. Customer 31 then requested that Crown Perth transfer the funds, together with his recent winnings and commission, to his foreign personal bank account: SMR dated 26 November 2014.

Due diligence

In November 2014, Customer 31's SMR history was reviewed by Crown Perth at the ML/TF Compliance Officer meeting, and a decision was made to continue rating Customer 31's risk as low. This was the only due diligence conducted by 1 March 2016.

1443. On and from November 2017, Customer 31 should have been recognised by Crown Melbourne as a high risk customer for the reasons pleaded at paragraphs 1442, 1447, 1448, 1449 and 1454.

Particulars

Section 36(1)(a), (b) of the Act and Chapter 15 of the Rules.

1444. At no point did Crown Melbourne assess Customer 31 high risk.

Particulars

On various occasions between 5 September 2011 and 23 November 2016, Crown Melbourne rated Customer 31 as low risk.

At no point did Crown Melbourne assess Customer 31 high risk.

This was despite Customer 31's significant turnover at Crown Melbourne. Between 18 November 2017 and 20 November 2017 alone, Customer 31 had a turnover that exceeded $84,000,000 with a win of $337,000 at Crown Melbourne.

See paragraph 120.

1445. As at 1 March 2016, Customer 31 should have been recognised by Crown Perth as a high risk customer for the reasons pleaded at paragraph 1442. At all times on and from 1 March 2016, Customer 31 should have been recognised by Crown Perth as a high risk customer for the reasons pleaded at paragraphs 1442, 1447, 1448, 1449, 1451 and 1454.

Particulars

Section 36(1)(a), (b) of the Act and Chapter 15 of the Rules.

1446. It was not until 13 May 2021 that Crown Perth rated Customer 31 high risk.

Particulars

On various occasions between 24 November 2014 and 12 May 2021, Crown Perth rated Customer 31 as low risk.

On 13 May 2021, Crown Perth rated Customer 31 high risk for the first time.

This was despite the transactions indicative of the ML/TF typology of cuckoo smurfing in 2014.

See paragraph 120.

1447. On and from 1 March 2016 designated services provided to Customer 31 posed higher ML/TF risks including because the provision of designated services to Customer 31 involved a combination of the following factors:

a. Customer 31 received high value financial (table 1, s6) and gaming services (table 3, s6);

b. Customer 31 was a foreign PEP: see paragraphs 118 and 663;

c. by no later than July 2018, Customer 31 had a turnover of $265,367,100 with a loss of $10,116,350 at Crown Melbourne. By no later than 2020, Customer 31 had a cumulative loss of $27,838,262 at Crown Perth;

d. Customer 31 and persons associated with him, transacted using large amounts of cash;

e. Customer 31 and persons associated with him engaged in transactions indicative of the ML/TF typology of cuckoo smurfing;

f. large values were transferred to Customer 31's bank accounts and his DAB account, and to and from other customers' DAB accounts, involving the provision by Crown Melbourne and Crown Perth of designated services within the meaning of items 31 and 32, table 1, s6 of the Act: see paragraph 411ff;

g. at various times, Customer 31 was provided with significant amounts of credit upon request, up to limits of $5,000,000: see paragraph 280ff;

h. by 2009, open sources made public allegations that Customer 31 was part of a crime syndicate that oversaw the majority of prostitution, gambling, narcotics, extortion and smuggling in a foreign country;

i. by November 2020, Crown Melbourne and Crown Perth were aware that Customer 31 was alleged to be a foreign 'crime lord'; and

j. by reason of the matters set out at subparagraphs a. to i. above, there were real risks that Customer 31's source of wealth and source of funds were not legitimate.

Monitoring of Customer 31's transactions

1448. At no time did Crown Melbourne or Crown Perth appropriately monitor Customer 31's transactions on a risk-basis.

Particulars

Section 36(1)(a), (b) of the Act and rules 15.4 to 15.8 of the Rules.

Crown Melbourne and Crown Perth did not apply appropriate risk-based transaction monitoring to designated services provided to Customer 31: see paragraphs 629 to 642 (designated services).

Customer 31's transactions involved repeated transactions indicative of ML/TF typologies and vulnerabilities that were not detected prior to a 2021 lookback. Had appropriate risk-based transaction monitoring been applied, these transactions could have been identified earlier: see paragraphs 686 and 687.

It was not until 2021 that Crown Perth identified transactions indicative of cuckoo smurfing that occurred between 3 October 2014 and 14 November 2014 totalling $2,416,864: see particulars to paragraph 1442. Crown Perth accepted that all deposits were made for the benefit of Customer 31. The funds were used to partly redeem Customer 31's credit markers totalling $6,181,100.

Transactions involving Customer 31 were identified as indicative of the ML/TF typology of large account balance by an independent auditor in 2021. By 30 April 2021, Customer 31's safekeeping account at Crown Melbourne had a balance at $4,700,000 that had been dormant for 217 days.

Ongoing customer due diligence

1449. On and from 1 March 2016, on multiple occasions, the provision of designated services to Customer 31 by Crown Melbourne and Crown Perth raised red flags reflective of higher ML/TF risks as a result of his individual and junket activity, which involved high losses.

Particulars

See paragraph 477.

Between 18 November 2017 and 20 November 2017 alone, Customer 31 had a turnover that exceeded $84,000,000 with a win of $337,000 at Crown Melbourne.

By July 2018, Crown Melbourne recorded Customer 31's individual gaming activity as a cumulative turnover of $265,367,100 with a loss of $10,116,350.

In FY2018, Crown Melbourne recorded Customer 31's individual gaming activity as cumulative turnover of $88,480,000 with a win of $337,500.

Crown Perth recorded Customer 31's individual rated gaming activity as:

- in 2016, a loss of $650,500;
- in 2018, a loss of $8,241,500;
- in 2017, a win of $8,506,500; and

- in 2019, a loss of $9,416,000.

By June 2019, Customer 31 had a debt to Crown Perth of approximately $4,500,000 due on 24 June 2019.

By March 2020, Crown Melbourne and Crown Perth had approved a CCF limit for Customer 31 of $5,000,000.

1450. At no time did Crown Melbourne or Crown Perth undertake appropriate risk-based customer due diligence with respect to Customer 31 with a view to identifying, mitigating and managing the ML/TF risks posed by the provision of designated services on and from 1 March 2016:

a. Crown Melbourne and Crown Perth did not take appropriate steps to analyse the information available to them regarding Customer 31's source of wealth/funds to determine whether the source of wealth/funds was legitimate in circumstances where he had previously been arrested in connection with bribery charges and was alleged to oversee the majority of prostitution, gambling, narcotics, extortion and smuggling in a foreign country; and

b. At no time did senior management consider whether continuing the business relationship with Customer 31 was within Crown Melbourne or Crown Perth's ML/TF risk appetite.

Particulars

Section 36(1)(a) of the Act.

The due diligence steps taken with respect to Customer 31 included:

Wealth and risk intelligence reports

Between November 2016 and August 2021, Crown Melbourne and Crown Perth conducted open source, risk intelligence and company searches and obtained wealth reports in respect of Customer 31 which identified his substantial personal wealth and business interests. The reports also identified allegations that Customer 31 bribed a government officer to withdraw a court case against Customer 31's business partner.

In October 2018, November 2020 and June 2021, Crown Melbourne and Crown Perth obtained a risk intelligence report in respect of Customer 31 which identified:

- Customer 31's arrest in respect of bribery charges in 2002 and subsequent acquittal;
- that Customer 31 was a foreign PEP due to his directorship position in a state-owned enterprise;
- that in 2009 Customer 31 was alleged to be a 'crime lord'; and

that Customer 31 was one of four men who oversaw the majority of prostitution, gambling, narcotics, extortion and smuggling in the country.

Senior management engagement

On 13 May 2020, a Vice President (International Business Operations) completed due diligence in respect of Customer 31 and

noted that she was unaware of any adverse information about Customer 31. This is despite the various adverse media reports identified to that date.

2021 reviews and lookback

In April 2021, Customer 31's personal assistant contacted Crown Perth regarding repayment of Customer 31's outstanding CCF debt, being approximately $4,500,000 due on 24 June 2019. The Group Chief Compliance and Financial Crime Officer (Crown Resorts) was satisfied that there was low risk associated with accepting the funds and the repayment should come from account(s) in Customer 31's name only or from companies beneficially owned by Customer 31, and be in the form of an IFTI.

In June 2021, the SPR process was applied in respect of Customer 31: see particulars to paragraph 1234.

None of these steps were proportionate to the ML/TF risks reasonably posed by Customer 31 on and 1 March 2016.

Enhanced customer due diligence

1451. Having formed a suspicion for the purposes of s41 of the Act, Crown Perth gave the AUSTRAC CEO an SMR with respect to Customer 31 on 19 May 2021.

Particulars

The SMR described the potential cuckoo smurfing that occurred in October and November 2014: see particulars to paragraph 1442.

1452. On each occasion that Crown Perth formed a suspicion with respect to Customer 31 for the purposes of s41 of the Act, it was required to apply its ECDD program to Customer 31.

Particulars

Rule 15.9(3) of the Rules.

1453. Crown Perth did not carry out appropriate risk-based ECDD measures with respect to Customer 31 following the submission of the SMR on 19 May 2021.

a. Appropriate risk-based steps were not taken to analyse information obtained by Crown Perth regarding Customer 31's source of wealth/funds or to determine the legitimacy of his source of wealth/funds.

b. Appropriate risk-based steps were not taken to analyse and monitor Customer 31's transactions – both past and future – including to understand their economic purpose. It was not until 2021 that the possible cuckoo smurfing in 2014 was identified: see paragraph 590 and 666.

c. At no time did senior management consider whether continuing the business relationship with Customer 31 was within Crown Perth's ML/TF risk appetite.

Particulars

Rules 15.9(3), 15.10(1)(c), (d), (2), (5) and (6) of the Rules.

Following the SMR given to the AUSTRAC CEO on 19 May 2021, Crown Perth conducted ECDD by carrying out risk intelligence and open source media searches and obtaining a risk intelligence report which, among other things, identified Customer 31 to be a foreign PEP and included allegations that Customer 31 was a 'crime lord'.

1454. At all times from 1 March 2016, Customer 31 was a foreign PEP.

Particulars

Customer 31 was a foreign PEP on the basis that he held a directorship position in a foreign state-owned enterprise.

1455. At all times from 1 March 2016, Crown Melbourne and Crown Perth was required to apply its ECDD program to Customer 31.

Particulars

Rules 15.9(2), 15.11 of the Rules.

See paragraphs 660, 663 and 666.

1456. Crown Melbourne and Crown Perth did not carry out appropriate risk-based ECDD measures with respect to Customer 31 on and from 1 March 2016 given his status as a foreign PEP. In particular:

a. Crown Melbourne did not undertake a detailed analysis of Customer 31's KYC information, nor did it take reasonable measures to identify Customer 31's source of wealth/funds;

b. senior management approval for Crown Melbourne to continue a business relationship with Customer 31 did not give adequate consideration to the ML/TF risks posed by the customer; and

c. senior management approval for Crown Melbourne to continue to provide designated services to Customer 31 did not give adequate consideration to the ML/TF risks posed by the customer.

Particulars

Rules 15.10(2), 15.10(6), 15.11 of the Rules.

See paragraphs 1450 and 1453.

See paragraph 660, 663, 666, 667 and 668.

1457. By reason of the matters pleaded from paragraphs 1438 to 1456, on and from 2017, Crown Melbourne:

a. did not monitor Customer 31 in relation to the provision of designated services, with a view to identifying, mitigating and managing the ML/TF risks it reasonably faced; and

b. did not do so in accordance with rr 15.5 and 15.9 of the Rules.

1458. By reason of the matters pleaded at paragraph 1457, Crown Melbourne contravened s36(1) of the Act on and from 2017 with respect to Customer 31.

Particulars

Section 36(1) of the Act is a civil penalty provision: s36(2) of the Act.

1459. By reason of the matters pleaded from 1438 to 1456, on and from 1 March 2016, Crown Perth:

a. did not monitor Customer 31 in relation to the provision of designated services, with a view to identifying, mitigating and managing the ML/TF risks it reasonably faced; and

b. did not do so in accordance with rr 15.5 and 15.9 of the Rules.

1460. By reason of the matters pleaded at paragraph 1459, Crown Perth contravened s36(1) of the Act on and from 1 March 2016 with respect to Customer 31.

Particulars

Section 36(1) of the Act is a civil penalty provision: s36(2) of the Act.

Customer 32

1461. Customer 32 has been a customer of Crown Melbourne from 24 June 2008 to 2 November 2020.

1462. From at least 27 June 2008 to 2 November 2020, Crown Melbourne provided Customer 32 with designated services within the meaning of table 3, s6 of the Act.

Particulars

Customer 32 was registered at Crown Melbourne on 24 June 2008.

Crown Melbourne issued Customer 32 with a WOL that was in place from 2 March 2015 to 20 September 2017.

On 2 November 2020, Crown Melbourne issued a second WOL in respect of Customer 32.

1463. From at least 12 December 2011, Customer 32 received designated services as a junket player, facilitated through two different junket operators.

Particulars

Customer 32 received designated services as a junket player under junkets operated by Customer 16 (or his predecessor) and another junket.

Between 2011 and 2018, Crown Melbourne recorded Customer 32's cumulative gaming activity at Crown Melbourne to be a turnover of $158,820,000 with $6,150,000 in losses and $522,850 in wins.

1464. Customer 32 has been a customer of Crown Perth from 26 June 2008 to 3 November 2021.

1465. From at least 26 June 2008 to 3 November 2021, Crown Perth provided Customer 32 with designated services within the meaning of table 3, s6 of the Act.

Particulars

On 3 November 2021, Crown Perth banned Customer 32 from attending its premises and issued an NRL.

1466. From at least 26 June 2008, Customer 32 received designated services as a junket player, facilitated through two different junket operators.

Particulars

Customer 32 received designated services as a junket player under the junket operated by Customer 16 (or his predecessor) and another junket.

Between 2008 and 2018, Customer 32 participated in 30 junket programs operated by Customer 16 (or his predecessor) at Crown Perth.

Between 2008 and 2018, Crown Melbourne recorded Customer 32's cumulative gaming activity at Crown Perth to be a turnover of $765,230,600 with losses of $12,225,050 and wins of $7,556,750.

The ML/TF risks posed by Customer 32

1467. By 1 March 2016, higher ML/TF risks were indicated by the nature and purpose of Customer 32's business relationship with Crown Melbourne and Crown Perth, the nature of the transactions he had been conducting, together with the suspicions Crown Melbourne itself had formed with respect to Customer 32.

Particulars

Section 36(1)(a), (b) of the Act and Chapter 15 of the Rules.

Customer 32 was a junket player. He received designated services through the channel of junket programs. This channel lacked transparency: see paragraph 477.

SMRs by 1 March 2016

By 1 March 2016, Crown Melbourne had given the AUSTRAC CEO two SMRs in relation to Customer 32 on 9 January 2012 and 23 December 2013. The SMRs reported suspicions in relation to high wins of $522,850 and losses of $4,022,050 by Customer 32 under junket programs run by Customer 16 (or his predecessor).

Gaming activity by 1 March 2016

By 1 March 2016, Customer 32's cumulative gaming activity at Crown Melbourne involved turnover of $123,160,000 with wins of $522,850 and losses of $4,020,000.

By 1 March 2016, Customer 32's cumulative gaming activity at Crown Perth was $593,620,600 with wins of $5,794,910 and losses of $10,770,000.

Open source information by 1 March 2016

By 1 March 2016, the following information on Customer 32 was available on open source databases:

- from 2001, Customer 32 was the subject of a United Nations Security Council Resolution in relation to logging activities by his company, which was given concessions by a former foreign political leader who was subsequently convicted of war crimes;

- from 2004 to 2015, Customer 32 was on a United Nations Security Council Committee sanctions list, which prevented him from travelling and froze his assets, following findings Customer 32 was an arms dealer who provided military and financial support to a former foreign political leader, assisting in destabilising a foreign company and gaining access to illicit diamonds;
- in 2005, Customer 32 was subject to a standing six-month jail term by a foreign court for contempt of court in relation to a financial fraud suit in 2004; and
- in 2014, Customer 32's associates were charged by a foreign government for breaching United Nations assets freezing prohibitions by paying Customer 32's bills and providing him with a credit card for use in the name of the associates.

Due diligence conducted by 1 March 2016

At no time from 2008 and 2015 did Crown Melbourne or Crown Perth perform any due diligence searches with respect to Customer 32.

Between February 2015 and 1 March 2016, the due diligence steps taken with respect to Customer 32 included:

- by at least 24 February 2015, Crown Perth performed a risk intelligence search on Customer 32, which reported that Customer 32 was reportedly an arms dealer who had been subject to a UN travel ban since 2004, and was subject to sanctions by eight foreign governments and international organisations. The results of the search were provided to the Group Executive General Manager – VIP International and Chief Legal Officer.
- on 27 February 2015, Crown Melbourne rated Customer 32 high risk and requested that stop codes be placed on Customer 32's accounts. On 2 March 2015, Crown Melbourne issued a WOL in respect of Customer 32.
- on 27 February 2015, Crown Perth did not issue an NRL but informed Customer 32 that it was unable to accept his business.

1468. Crown Melbourne first rated Customer 32's risk as high on 27 February 2015.

Particulars

On two occasions between 9 January 2012 and 23 December 2013, Crown Melbourne assessed Customer 32 as moderate risk.

On nine occasions between 27 February 2015 and 20 January 2021, Crown Melbourne assessed Customer 32 as high risk.

See paragraph 481.

1469. Crown Perth first rated Customer 32's risk as high on 27 February 2015.

Particulars

On 20 February 2015, Crown Perth assessed Customer 32 as low risk.

On four occasions between 27 February 2015 and 20 January 2021, Crown Perth assessed Customer 32 as high risk.

See paragraph 481.

1470. On and from 1 March 2016, designated services provided to Customer 32 posed higher ML/TF risks including because the provision of designated services to Customer 32 involved a combination of the following factors:

a. Customer 32 received high value gaming services (table 3, s6) provided through multiple junket programs;

b. Customer 32 was a junket player;

c. Customer 32 was a foreign PEP: see paragraphs 118 and 663;

d. by no later than 3 May 2018, Crown Melbourne recorded that Customer 32's turnover under Customer 16's (or his predecessor's) junket at Crown Melbourne on and from 1 March 2016 had exceeded $34,660,000;

e. by no later than 19 August 2018, Crown Perth recorded that Customer 32's turnover under Customer 16's (or his predecessor's) junket at Crown Perth on and from 1 March 2016 had exceeded $171,610,000;

f. designated services provided to Customer 32 lacked transparency as the services were provided through the channel of junket programs: see paragraph 477(e);

g. the table 3, s6, designated services provided to Customer 32 involved high turnover;

h. Customer 32 also engaged in other transactions indicative of ML/TF typologies and vulnerabilities, including cashing-in large value chips with no evidence of play: see paragraph 24;

i. these transactions took place against the background of:

i. open source information being available from 2001 indicating that Customer 32 was the subject of a United Nations Security Council Resolution in relation to logging activities by his company, which was given concessions by a former foreign political leader who was subsequently convicted of war crimes;

ii. open source information being available from at least 2011 stating that Customer 32 was on a UN sanctions list following findings that he was an arms dealer who provided military and financial support to a former foreign political leader, assisting in destabilising a foreign company and gaining access to illicit diamonds;

iii. Crown Melbourne and Crown Perth being aware that the United Nations Security Council Committee had sanctioned Customer 32 from 2004 to 2015, after making findings that he was an arms dealer who provided military and financial support to a former foreign political leader who was subsequently convicted of war crimes;

iv. Crown Melbourne and Crown Perth being aware of Customer 32's conviction and imposition of a standing six-month jail term for contempt of court in financial fraud proceedings in a foreign jurisdiction in 2005;

v. two SMRs being given to the AUSTRAC CEO by Crown Melbourne by 1 March 2016; and

j. by reason of the matters set out at subparagraphs a. to i. above, there were real risks that Customer 32's source of wealth/funds were not legitimate.

Monitoring of Customer 32's transactions

1471. At no time did Crown Melbourne and Crown Perth appropriately monitor Customer 32's transactions on a risk-basis.

Particulars

Section 36(1)(a), (b) of the Act and rules 15.4 to 15.8 of the Rules.

Crown Melbourne and Crown Perth were unable to monitor the ML/TF risks posed by Customer 32's transactions appropriately because they did not make and keep appropriate records of designated services provided to junket players: see paragraphs 483ff.

Crown Melbourne and Crown Perth did not apply appropriate risk-based transaction monitoring to designated services provided to Customer 32: see paragraphs 590ff, 629 to 642 and 643 to 649.

Ongoing customer due diligence

1472. On and from August 2017, on multiple occasions, the provision of designated services to Customer 32 by Crown Melbourne and Crown Perth raised red flags reflective of higher ML/TF risks as a result of:

a. his junket play including his high turnover; and

b. suspicious transactions including exchanging chips with no evidence of play.

Particulars

See paragraph 477.

By August 2017, Crown Perth determined that it would resume business with Customer 32, following receipt of information indicating that Customer 32 was no longer subject to UN sanctions.

On 20 September 2017, Crown Melbourne revoked the WOL applicable to Customer 32, and removed stop codes on Customer 32's accounts.

2017 junket activity (Crown Perth)

Between 18 August 2017 and 21 August 2017, Customer 32 attended Crown Perth as part of the Customer 16 junket. Crown Perth recorded his turnover was $17,450,000 with wins of $567,650.

Between 19 September 2017 and 25 September 2017, Customer 32 attended Crown Perth as part of the Customer 16 junket. Crown Perth recorded his turnover was $27,320,000 with losses of $1,030,000.

Between 6 October 2017 and 9 October 2017, Customer 32 attended Crown Perth as part of the Customer 16 junket. Crown Perth recorded his turnover was $17,000,000 with losses of $60,200.

Between 30 December 2017 and 3 January 2018, Customer 32 attended Crown Perth as part of the Customer 16 junket. Crown Perth recorded his turnover was $38,290,000 with wins of $722,550.

Crown Perth recorded that Customer 32's gaming activity at Crown Perth in 2017 involved total turnover of $100,060,000, with wins of $1,290,200 and losses of $1,090,200.

2018 junket activity (Crown Melbourne)

From 3 May 2018 to 17 May 2018, Customer 32 attended Crown Melbourne as part of the Customer 16 junket. Crown Melbourne recorded his turnover was approximately $34,660,000 with losses of approximately $2,130,000.

By 9 May 2018, Crown Melbourne had formed suspicions with respect to high losses of $2,134,700 noted for Customer 32 under the Customer 16 junket, and had given the AUSTRAC CEO an SMR in respect of the activity: SMR dated 9 May 2018.

2018 junket activity (Crown Perth)

On 1 January 2018, Crown Perth made Customer 32 a VIP, high roller, and/or premium program player.

Between 22 June 2018 and 25 June 2018, Customer 32 attended Crown Perth as part of the Customer 16 junket. Crown Perth recorded his turnover was $14,570,000 with wins of $471,640.

Between 19 August 2018 and 22 August 2018, Customer 32 attended Crown Perth as part of the Customer 16 junket. Crown Perth recorded his turnover was $56,980,000 with losses of $364,850.

Crown Perth recorded that Customer 32's gaming activity at Crown Perth in 2018 involved total turnover of $71,550,000 with wins of $471,640 and losses of $364,850.

Unusual transactions in 2019 (Crown Melbourne)

On 16 June 2019, Customer 32 exchanged $11,000 in gaming chips for cash, despite not having any recorded play: SMR dated 18 June 2019.

1473. At no time did Crown Melbourne or Crown Perth undertake appropriate risk-based customer due diligence with respect to Customer 32 with a view to identifying, mitigating and managing the ML/TF risks posed by the provision of designated services on and from 1 March 2016:

a. at no time did Crown Melbourne or Crown Perth take appropriate steps to understand Customer 32's source of wealth/funds was legitimate;

b. at no time did Crown Melbourne or Crown Perth take appropriate steps to identify or analyse the ML/TF risks of Customer 32's transactions or to consider whether they had a lawful purpose;

c. at no time did Crown Melbourne or Crown Perth give appropriate consideration to whether large and high risk transactions should be processed;

d. After the decision to revoke the WOL in respect of Customer 32 in November 2017 and until to the decision to issue Customer 32 with a WOL in November 2020, there is no record of senior management considering whether continuing the business relationship with Customer 32 was within Crown Melbourne's ML/TF risk appetite in light of the ML/TF risks posed by Customer 32.

e. After the decision to revoke the NRL in respect of Customer 32 in August 2017 and until to the decision to issue Customer 32 with a WOL in November 2021, there is no record of senior management considering whether continuing the business relationship with Customer 32 was within Crown Perth's ML/TF risk appetite in light of the ML/TF risks posed by Customer 32. Crown Perth issued Customer 32 with an NRL a year after Crown Melbourne issued him with a WOL and ten months after the POI Committee determined to issue a WOL in respect of Customer 32.

Particulars

Section 36(1)(a) of the Act.

Senior management at Crown Melbourne failed to adequately consider whether a business relationship with Customer 32 was within its ML/TF risk appetite until 2 November 2020.

Senior management at Crown Perth failed to adequately consider whether a business relationship with Customer 32 was within its ML/TF risk appetite until 20 January 2021, and did not issue an NRL until 3 November 2021.

The due diligence steps taken with respect to Customer 32 included:

Database searches

On 3 August 2017, 4 August 2017, 7 August 2017, 22 September 2017, 30 April 2018, 17 October 2019, Crown performed risk intelligence searches on Customer 32.

Between 3 August and 9 August 2019, Crown performed various company and property searches on companies and properties associated with Customer 32.

Player profile

By 18 September 2017, the Credit control team prepared a player profile using the information obtained in database searches conducted in August 2017. The profile:

- summarised findings of risk intelligence searches which reported that Customer 32 was an arms dealer connected to a foreign political leader convicted of war crimes, but that sanctions against him had been lifted in 2015;
- summarised the findings of the wealth reports obtained on Customer 32 which reported that:

- Customer 32 was a PEP by association on the basis of his association with a former political leader who was subsequently convicted of war crimes in 2012;
- Customer 32 was subject to sanctions between 2004 and 2015, was the CEO of Company 8, which was used by the former foreign political leader to smuggle weapons and fund war crimes. The company's chairman was subsequently convicted of war crimes and arms trafficking in 2017; and
- Customer 32's associates had been fined by a foreign government in 2014 for providing financial assistance (including paying off credit card and golf membership bills) to Customer 32 during the period in which sanctions applied to him;

- set out Customer 32's present directorships and shareholdings; and
- summarised findings from open source media searches conducted on 9 August 2017:
  - a blog post published on 8 February 2017, which reported that a trial of the chairman of Company 8 (of which Customer 32 was CEO) for war crimes had been reopened; and
  - an article published on 22 April 2017, which reported that the chairman of Company 8 (of which Customer 32 was CEO) had been convicted of war crimes and arms trafficking.

Senior management engagement

Between 2016 and September 2017, Crown senior management engaged with Customer 32's lawyers regarding the removal of Customer 32's WOL at Crown Melbourne and resumption of business at Crown Perth. Customer 32's lawyers provided copies of letters from foreign governments that indicated that Customer 32 was no longer sanctioned by the United Nations.

In July and August 2017, the Chief Legal Officer (Australian Resorts), Legal Officer (AML), CTRM, and the Group Executive General Manager (Regulatory and Compliance) each considered Crown's relationship with Customer 32.

By August 2017, senior management at Crown Perth had determined that it would resume business with Customer 32, following receipt of information indicating that Customer 32 was no longer subject to UN sanctions.

By 19 September 2017, following the preparation of the player profile, Crown senior management, including the Chief Executive Officer

(Crown Resorts) and the AML Committee approved lifting Customer 32's WOL at Crown Melbourne.

On 29 August 2018, Customer 32's profile was considered by the Fortnightly AML/CTF Officer Meeting at Crown Perth. No further action was taken.

By 2 January 2019, the Group General Manager (AML) reviewed Customer 32's profile. No further action was taken.

On 2 November 2020, the Group General Manager (Regulatory and Compliance) directed Crown Melbourne to issue a WOL in respect of Customer 32, which took effect on the same day.

January 2021 POI Committee and WOL

On 20 January 2021, the Crown Resorts POI Committee considered Customer 32, who had come to the Committee's attention through the ILGA inquiry. The Committee agreed to issue a WOL in respect of Customer 32, if one had not been issued already.

April 2021 – VCGLR Show Cause Decision

By 27 April 2021, the VCLGR reached a decision on the show cause notice it had issued under section 20(2) of the *Casino Control Act 1991* (Vic) with respect to Customer 32, which alleged that Crown Melbourne had breached the Act by allowing Customer 32 to gamble despite being subject to sanctions, and by failing to conduct sufficient probity checks including into his conviction and imprisonment for 6 months in 2005 for failure to disclose asset information. The show cause notice also referred to other individuals, including Customer 1, Customer 2 and Customer 26 . The VCGLR concluded that Crown Melbourne had breached s121(4) of the *Casino Control Act 1991* (Vic) and imposed the maximum fine of $1,000,000.

On 3 November 2021, Crown Perth issued an NRL in respect of Customer 32.

At no time between 2017 and 2020 did senior management give adequate consideration to the ML/TF risks posed by Customer 32 and whether an ongoing business relationship was within Crown Melbourne's ML/TF risk appetite.

At no time between 2017 and 2021 did senior management give adequate consideration to the ML/TF risks posed by Customer 32 and whether an ongoing business relationship was within Crown Perth's ML/TF risk appetite.

Prior to the issue of the WOL/NRL, none of the due diligence steps taken by Crown Melbourne or Crown Perth were proportionate to the ML/TF risks reasonably posed by Customer 32 on and from 1 March 2016.

1474. From 1 March 2016, a number of widely accessible media reports were published in respect of Customer 32. These articles do not appear to have come to Crown's attention as part of its due diligence process.

Particulars

Additional media reports concerned sanctions imposed on Customer 32 between 2004 and 2015 in respect of activities involving Company 8 and a former foreign political leader, subsequently convicted of war crimes. The articles referred to findings by the UN Security Council Committee that Customer 32 was an arms dealer who provided military and financial support to a former foreign political leader, assisting in destabilising a foreign company and gaining access to illicit diamonds.

An article from 2009 reported that in 2005 Customer 32 was subject to a standing six-month jail term by a foreign court for contempt of court in relation to a financial fraud suit in 2004.

In October 2019, Australian media reports alleged that Crown Melbourne and Crown Perth had hosted Customer 32 and permitted him to gamble during the period when he was subject to UN sanctions, including a travel ban and asset freezing.

Enhanced customer due diligence

1475. Having formed a suspicion for the purposes of s41 of the Act, Crown Melbourne gave the AUSTRAC CEO an SMR with respect to Customer 32 on 9 May 2018.

Particulars

The SMR reported high losses noted for Customer 32 under a Customer 16 junket program.

1476. On each occasion that Crown Melbourne formed a suspicion with respect to Customer 32 for the purposes of s41 of the Act, it was required to apply its ECDD program to Customer 32.

Particulars

Rule 15.9(3) of the Rules.

1477. Crown Melbourne did not carry out appropriate risk-based ECDD measures with respect to Customer 32 on each occasion that Crown Melbourne formed a suspicion with respect to Customer 32 for the purposes of s41 of the Act.

a. There are no records of ECDD being conducted following the lodgement of the SMR on 9 May 2018: see paragraphs 664 and 685.

b. Appropriate risk-based steps were not taken to obtain or analyse information about Customer 32's source of funds for the transaction that gave rise to Crown Melbourne's suspicion reported in the SMR dated 9 May 2018: see paragraph 667.

c. Appropriate risk-based steps were not taken to analyse and monitor Customer 32's transactions – both past and future – including to understand their economic purpose: see paragraph 590 and 666.

d. After the decision to revoke the WOL in respect of Customer 32 in November 2017 and until to the decision to issue Customer 32 with a WOL in November 2020, there is no record of senior management considering whether continuing the business relationship with Customer 32 was within Crown Melbourne's ML/TF risk appetite in light of the ML/TF risks posed by Customer 32:

i. in 2017, senior management decided to lift the WOL that was in place in respect of Customer 32 at Crown Melbourne. At the time this decision was made, Crown held information summarised in the 2017 junket profile, including his association with a company whose chairman had been convicted of war crimes and arms trafficking, and the fact that his associates had been fined for providing financial assistance to him whilst he was subject to UN sanctions;

ii. following the decision to accept Customer 32's business in 2017 until late 2020, Crown senior management considered Customer 32's customer profile twice for the purpose of assessing ML/TF risk; and

iii. it was not until November 2020, when Customer 32's customer profile was reviewed by senior management for the third time since re-commencing business with him that Crown senior management made the decision that a business relationship with Customer 32 was no longer within Crown Melbourne's ML/TF risk appetite. No new information had been obtained by Crown prior to this decision being made.

Particulars

Rules 15.9(3), 15.10(1)(c), (d), (2), (5) and (6) of the Rules.

See particulars to paragraph 1473.

1478. Having formed a suspicion for the purposes of s41 of the Act, Crown Perth gave the AUSTRAC CEO an SMR with respect to Customer 32 on 18 June 2019.

Particulars

The SMR reported an exchange of chips for cash not supported by recorded gaming.

1479. On each occasion that Crown Perth formed a suspicion with respect to Customer 32 for the purposes of s41 of the Act, it was required to apply its ECDD program to Customer 32.

Particulars

Rule 15.9(3) of the Rules.

1480. Crown Perth did not carry out appropriate risk-based ECDD measures with respect to Customer 32 on each occasion that Crown Perth formed a suspicion with respect to Customer 32 for the purposes of s41 of the Act.

a. There are no records of ECDD being conducted following the lodgement of the SMR on 18 June 2019: see paragraphs 664 and 685.

b. Appropriate risk-based steps were not taken to obtain or analyse information about Customer 32's source of funds for the transaction that gave rise to Crown Perth's suspicion reported in the SMR dated 18 June 2019: see paragraph 667.

c. Appropriate risk-based steps were not taken to analyse and monitor Customer 32's transactions – both past and future – including to understand their economic purpose: see paragraph 590 and 666.

d. After the decision to revoke the NRL in respect of Customer 32 in August 2017 and until to the decision to issue Customer 32 with a WOL in November 2021, there is no record of senior management considering whether continuing the business relationship with Customer 32 was within Crown Perth's ML/TF risk appetite in light of the ML/TF risks posed by Customer 32. Crown Perth issued Customer 32 with an NRL a year after

Crown Melbourne issued him with a WOL and ten months after the POI Committee determined to issue a WOL in respect of Customer 32:

i. in 2017, senior management at Crown Perth decided to resume doing business with Customer 32. At the time this decision was made, Crown held information summarised in the 2017 junket profile, including his association with a company whose chairman had been convicted of war crimes and arms trafficking, and the fact that his associates had been fined for providing financial assistance to him whilst he was subject to UN sanctions;

ii. following the decision to accept Customer 32's business in 2017 until late 2020, Crown senior management considered Customer 32's customer profile twice for the purpose of assessing ML/TF risk; and

iii. notwithstanding that Crown Melbourne issued Customer 32 with a WOL in November 2020, Crown Perth did not issue Customer 32 with an NRL until November 2021, almost six months after Crown Melbourne had been fined $1,000,000 by the VCGLR for, among other things, failing to conduct sufficient probity checks in respect of Customer 32. There are no records of any senior management consideration of Customer 32 in relation to the decision to issue him with an NRL.

Particulars

Rules 15.9(3), 15.10(1)(c), (d), (2), (5) and (6) of the Rules.

See particulars to paragraph 1473.

1481. At all times from 1 March 2016, Customer 32 was a foreign PEP.

Particulars

Section 36(1)(a) of the Act.

Customer 32 was a PEP by association on the basis of his association with a former political leader who was subsequently convicted of war crimes in 2012.

The wealth report dated 7 August 2017 identified Customer 32 as a PEP by association.

1482. At all times from 1 March 2016, Crown Melbourne and Crown Perth was required to apply its ECDD program to Customer 32.

Particulars

Rules 15.9(2), 15.11 of the Rules.

See paragraphs 660, 663 and 666.

1483. Crown Melbourne and Crown Perth did not carry out appropriate risk-based ECDD measures with respect to Customer 32 on and from 1 March 2016 given his status as a foreign PEP. In particular:

a. Crown Melbourne and Crown Perth did not undertake a detailed analysis of Customer 32's KYC information or analyse the legitimacy of Customer 32's source of wealth/funds;

b. no adequate steps were taken to seek and obtain senior management approval for continuing a business relationship with Customer 32 having regard to the ML/TF risks

posed by the customer in a way that considered the ML/TF risks associated with the customer; and

c. no adequate steps were taken to seek and obtain senior management approval for whether Crown Melbourne and Crown Perth should continue to provide designated services to Customer 32 in a way that considered the ML/TF risks associated with the customer.

Particulars

Rules 15.10(2), 15.10(6), 15.11 of the Rules.

See paragraphs 1477 and 1480.

See paragraph 660, 663, 666, 667 and 668.

1484. On and from 27 February 2015, Crown Melbourne and Crown Perth rated Customer 32 high risk.

Particulars

Crown Melbourne assessed Customer 32 high risk on nine occasions between 27 February 2015 and 20 January 2021: see paragraph 1468.

Crown Perth assessed Customer 32 high risk on four occasions between 27 February 2015 and 20 January 2021: see paragraph 1469.

1485. On each occasion that Crown Melbourne and Crown Perth rated Customer 32 high risk, Crown Melbourne and Crown Perth was required to apply its ECDD program to Customer 32.

Particulars

Rule 15.9(1) of the Rules.

See paragraph 661.

1486. Crown Melbourne and Crown Perth did not carry out appropriate risk-based ECDD measures with respect to Customer 32 on each occasion that Crown Melbourne and Crown Perth rated Customer 32 high risk.

Particulars

At no time did Crown Melbourne or Crown Perth conduct ECDD following each occasion that it rated Customer 32 high risk, despite the higher ML/TF risks known to Crown Melbourne and Crown Perth: See paragraphs 1477 and 1480.

See paragraphs 661, 666, 667 and 668.

1487. By reason of the matters pleaded from paragraphs 1461 and 1486, on and from August 2017, Crown Melbourne and Crown Perth:

a. did not monitor Customer 32 in relation to the provision of designated services, with a view to identifying, mitigating and managing the ML/TF risks it reasonably faced; and

b. did not do so in accordance with rr 15.5 and 15.9 of the Rules.

1488. By reason of the matters pleaded at paragraph 1487, Crown Melbourne contravened s36(1) of the Act on and from August 2017 to 2 November 2020 with respect to Customer 32.

Particulars

Section 36(1) of the Act is a civil penalty provision: s36(2) of the Act.

1489. By reason of the matters pleaded at paragraph 1487, Crown Perth contravened s36(1) of the Act on and from August 2017 to 3 November 2021 with respect to Customer 32.

Particulars

Section 36(1) of the Act is a civil penalty provision: s36(2) of the Act.

Customer 33

1490. Customer 33 has been a customer of Crown Melbourne since 28 November 2015.

1491. From at least 28 November 2015, Crown Melbourne provided Customer 33 with designated services within the meaning of table 1 and table 3, s6 of the Act.

1492. From at least February 2018, Customer 33 received designated services as a junket player, facilitated through two different junket operators.

Particulars to paragraphs 1491 and 1492

In and from February 2018, Customer 33 was a junket player with the Meg-Star and Customer 4 junket programs. Customer 33 attended Crown Melbourne as a junket player on at least three occasions.

On 28 November 2015, Customer 33 made a chip cash-in of $49,800 at Crown Melbourne.

On 11 December 2015, Crown Melbourne opened a DAB account and safekeeping account (AUD) for Customer 33, which remain open.

Between 2016 and August 2019, Crown Melbourne recorded Customer 33's individual rated gaming activity as cumulative loss of $7,107,860.

Between 28 February 2018 and 31 March 2019, Crown Melbourne recorded Customer 33's individual gaming activity and gaming activity on junket programs to be cumulative turnover of $37,290,300 and cumulative loss of $1,430,940.

The ML/TF risks posed by Customer 33

1493. By 1 March 2016 higher ML/TF risks were indicated by the nature and purpose of Customer 33's business relationship with Crown Melbourne, the nature of the transactions he had been conducting, together with the suspicions Crown Melbourne itself had formed with respect to Customer 33.

Particulars

Section 36(1)(a), (b) of the Act and Chapter 15 of the Rules.

By 1 March 2016, Crown Melbourne had given the AUSTRAC CEO five SMRs in relation to Customer 33 on 30 November 2015, 14

December 2015, 11 January 2016, 15 February 2016 and 23 February 2016. The SMRs reported Customer 33's individual annual losses, telegraphic transactions not supported by rated gaming activity, and significant third party telegraphic transfers.

Cash transactions by 1 March 2016

Between 28 November 2015 and 10 December 2015, Customer 33 made four chip cash-ins totalling $224,600.

On 12 December 2015, Customer 33 made a cash withdrawal of $120,000.

Third party transactions by 1 March 2016

On 8 January 2016, Customer 33 sent a telegraphic transfer of $1,000,000 to a third party This amount exceeded Customer 33's rated wins at that time: SMR dated 11 January 2016.

On 23 February 2016, Customer 33 sent a telegraphic transfer of $300,000 to a third party: SMR dated 23 February 2016.

Individual rated gaming activity by 1 March 2016

In 2015, Crown Melbourne recorded Customer 33's individual rated gaming activity as buy-in $2,476,350 and win $274,265.

Due diligence conducted by 1 March 2016

By 1 March 2016, despite Customer 33's significant individual gaming activity and large cash and third party transactions, no due diligence steps had been taken by Crown Melbourne in respect to Customer 33.

1494. As at 1 March 2016, Customer 33 should have been recognised by Crown Melbourne as a high risk customer for the reasons pleaded at paragraph 1493.

1495. At no time was Customer 33 rated high risk by Crown Melbourne

Particulars

On various occasions between 30 November 2015 and 8 August 2019, Crown Melbourne assessed Customer 33 to be moderate risk.

See paragraph 481.

1496. At all times on and from 1 March 2016, Customer 33 should have been recognised by Crown Melbourne as a high risk customer by reason of the matters pleaded at paragraphs 1493, 1497, 1499, 1500, 1501, 1502 and 1504.

Particulars

Section 36(1)(a), (b) of the Act and Chapter 15 of the Rules.

By 1 March 2016, Customer 33 had been the subject of five SMRs, had recorded significant individual rated gaming activity and had sent a telegraphic transfer of $1,000,000 to a third party. In 2016, Customer 33's buy-in had escalated from $2,476,350 to $22,537,700

and Customer 33's win/loss had escalated from a win of $274,265 to a loss of $3,579,895.

1497. On and from 1 March 2016 designated services provided to Customer 33 posed higher ML/TF risks including because the provision of designated services to Customer 33 involved a combination of the following factors:

a. Customer 33 was a junket player;

b. Customer 33 received high value financial (table 1, s6) and gaming services (table 3, s6) provided through the Meg-Star and Customer 4 junket programs: see paragraph 473ff;

c. between February 2018 and March 2019, Crown Melbourne recorded that Customer 33 had a junket and individual turnover that exceeded $37,000,000;

d. from 2018, Customer 33 was known to be connected to the Meg-Star junket operator, Customer 3, and another junket operator, Customer 4. Crown Melbourne had formed suspicions in respect of both these junket operators;

e. designated services provided to Customer 33 lacked transparency as the services were provided through the channel of junket programs: see paragraph 477(e);

f. customer 33 transacted using large amounts of cash;

g. between 2016 and 2019, Crown Melbourne recorded Customer 33's individual rated gaming activity to be a cumulative loss of $7,107,860;

h. designated services provided to Customer 33 involved large value transfers to and from third parties, including from the Meg-Star junket operator, Customer 3, and unknown third parties;

i. Customer 33 engaged in transactions indicative of ML/TF typologies and vulnerabilities including quick turnover of money (without betting): see paragraph 24;

j. these transactions took place against the background of:

   i. in January 2016, Customer 33 sent two telegraphic transfers of $1,000,000 and $300,000 respectively to third parties;

   ii. five SMRs being given to the AUSTRAC CEO by Crown Melbourne by 1 March 2016;

k. by 11 March 2016 Customer 33 had transacted $3,445,000 through HCT channel for redemption at Crown Melbourne during FY2016: see paragraphs 418, 419, 420 and 422; ands

l. by reason of the matters set out at subparagraphs a. to k. above, there were higher ML/TF risks associated with Customer 33's source of wealth/funds.

Monitoring of Customer 33's transactions

1498. At no time did Crown Melbourne appropriately monitor Customer 33's transactions on a risk-basis.

Particulars

Section 36(1)(a), (b) of the Act and rules 15.4 to 15.8 of the Rules.

Crown Melbourne was unable to monitor the ML/TF risks posed by Customer 33's transactions appropriately because it did not make and keep appropriate records of designated services provided to junket players: see paragraphs 483ff.

Crown Melbourne did not apply appropriate risk-based transaction monitoring to designated services provided to Customer 33: see paragraphs 590ff, 629 to 642 and 643 to 649.

Had appropriate risk-based transaction monitoring been applied, these transactions could have been identified earlier: see paragraph 686 and 687.

Ongoing customer due diligence

1499. On and from 1 March 2016, on multiple occasions, the provision of designated services to Customer 33 by Crown Melbourne raised red flags reflective of higher ML/TF risks as a result of his use of the HCT channel.

Particulars

See paragraphs 418, 419, 420 and 422.

Crown Melbourne engaged in a practice in which it would receive payment at Crown Towers Hotel from international VIP customers using a credit or debit card (ordinarily a foreign credit card). The funds were then made available to the customer for gaming at Crown Melbourne.

By 11 March 2016, Customer 33 had transferred $3,445,000 through the HCT channel in FY2016.

1500. On and from 1 March 2016, on multiple occasions, the provision of designated services to Customer 33 by Crown Melbourne raised red flags reflective of higher ML/TF risks as a result of large transactions which sometimes involved third parties.

Particulars

See paragraph 456ff.

Between 24 February 2017 and 8 March 2019, Customer 33 was involved in eight telegraphic transfers totalling $1,600,000. It is unclear from the SYCO records whether these telegraphic transfers were sent or received by Customer 33.

On 15 March 2019, the Meg-Star junket operator, Customer 3, deposited $210,000 into Customer 33's DAB account. Customer 33 withdrew these funds in the form of cash ($10,000) and chip purchase vouchers ($50,000, $50,000 and $100,000).

1501. On and from 1 March 2016, on multiple occasions, the provision of designated services to Customer 33 by Crown Melbourne raised red flags reflective of higher ML/TF risks as a result of his individual and junket gaming activity, which involved high turnover.

Particulars

See paragraph 477.

Individual gaming activity

In 2016, Crown Melbourne recorded Customer 33's individual rated gaming activity as buy-in $22,537,700 and loss $3,579,895. This was a significant escalation from 2015, in which Customer 33's buy-in was $2,476,350 and Customer 33 experienced a win of $274,265.

In 2017, Crown Melbourne recorded Customer 33's individual rated gaming activity as buy-in $6,814,800 and loss $2,505,430.

In 2018, Crown Melbourne recorded Customer 33's individual rated gaming activity as buy-in $568,200 and loss $555,505.

In 2019, Crown Melbourne recorded Customer 33's individual rated gaming activity as buy-in $666,000 and loss $467,030.

Junket activity

In February 2018, Customer 33 attended a Customer 4 junket program with a turnover of $27,720,000 with a loss of $71,790.

In February 2018, Customer 33 also attended a Meg-Star junket program with a turnover of $270,300 with a loss of $29,150.

In March 2019, Customer 33 attended a Meg-Star junket program with a turnover of $9,380,000 with a loss of $1,330,000.

Other red flags

Between 1 March 2016 and 5 March 2016, Customer 33 was involved in revenue deviation disputes in respect of his play of the table game baccarat. The deviation sums ranged from $200,000 to $1,548,600.

1502. On and from 1 March 2016, on multiple occasions, the provision of designated services to Customer 33 by Crown Melbourne raised red flags reflective of higher ML/TF risks as a result of large cash transactions.

Particulars

See paragraphs 450 and 451.

On 3 March 2016, Customer 33 made a cash deposit of $500,000 and a withdrawal of $300,000.

On 9 February 2017, Customer 33 made a cash withdrawal of $80,000 followed by an account deposit of $80,000 one minute later and a chip cash out of $60,000 on the same day. This transaction was indicative of the ML/TF typology of quick turnover (without betting).

On 13 February 2017, Customer 33 made a cash withdrawal of $50,000.

On 23 February 2017, Customer 33 made an account deposit of $30,000.

On 10 August 2018, Customer 33 made an account deposit of $50,000.

On 9 March 2019, Customer 33 made a cash withdrawal of $150,000.

1503. At no time did Crown Melbourne undertake appropriate risk-based customer due diligence with respect to Customer 33 with a view to identifying, mitigating and managing the ML/TF risks posed by the provision of designated services on and from 1 March 2016.

a. At no time did Crown Melbourne take appropriate steps to understand whether Customer 33's source of wealth/funds was legitimate.

b. At no time did Crown Melbourne take appropriate steps to identify or analyse the ML/TF risks of Customer 33's transactions or to consider whether they had a lawful purpose.

c. Crown Melbourne gave no consideration at any time to whether large and high risk transactions should be processed.

d. At no time did senior management consider whether continuing the business relationship with Customer 33 was within Crown Melbourne's ML/TF risk appetite.

Particulars

Section 36(1)(a) of the Act.

The due diligence steps taken with respect to Customer 33 included:

- on 31 January 2017 and 18 March 2019, Crown Melbourne conducted a risk intelligence search in respect of Customer 33;
- in January 2017, Crown Melbourne obtained wealth reports and conducted internet searches in respect of Customer 33;
- in March 2019, Crown Melbourne compiled its internal documents in respect of Customer 33 together with the risk intelligence searches conducted in March 2019 and wealth reports obtained in January 2017; and
- in August 2019, the Group General Manager (AML) asked the CTRM to examine the financial activity of Customer 33 together with Crown Melbourne's due diligence information to determine whether there was information relevant for disclosure under s41 of the Act. This resulted in an SMR being filed: see paragraphs: see paragraph 1504.

None of these steps were proportionate to the ML/TF risks reasonably posed by Customer 33 on and from 1 March 2016.

Enhanced customer due diligence

1504. Having formed a suspicion for the purposes of s41 of the Act, Crown Melbourne gave the AUSTRAC CEO SMRs with respect to Customer 33 on:

a. 7 March 2016;

b. 30 March 2016; and

c. 8 August 2019.

Particulars

The SMRs described Customer 33's individual and junket losses and the amount of cash Customer 33 was prepared to carry.

1505. On each occasion that Crown Melbourne formed a suspicion with respect to Customer 33 for the purposes of s41 of the Act, it was required to apply its ECDD program to Customer 33.

Particulars

Rule 15.9(3) of the Rules.

1506. Crown Melbourne did not carry out appropriate risk-based ECDD measures with respect to Customer 33 on each occasion that Crown Melbourne formed a suspicion with respect to Customer 33 for the purposes of s41 of the Act.

a. There are no records of ECDD being conducted following the lodgement of SMRs on 7 March 2016, 30 March 2016 and 8 August 2019: see paragraphs 664 and 685.

b. Appropriate risk-based steps were not taken to obtain or analyse information about Customer 33's source of wealth/funds: see paragraph 667.

c. Appropriate risk-based steps were not taken to analyse and monitor Customer 33's transactions – both past and future – including to understand their economic purpose: see paragraph 590 and 666.

d. At no time did senior management consider whether continuing the business relationship with Customer 33 was within Crown Melbourne's ML/TF risk appetite.

Particulars

Rules 15.9(3), 15.10(1)(c), (d), (2), (5) and (6) of the Rules.

Although the CTRM compiled Customer 33's internal Crown Melbourne files prior to giving the AUSTRAC CEO an SMR on 8 August 2019, no additional steps were taken to obtain or analyse information about Customer 33's source of wealth/funds: see particulars to paragraph 1503. ECDD was not conducted in respect of this SMR.

1507. By reason of the matters pleaded from paragraphs 1490 to 1506, on and from 1 March 2016, Crown Melbourne:

a. did not monitor Customer 33 in relation to the provision of designated services, with a view to identifying, mitigating and managing the ML/TF risks it reasonably faced; and

b. did not do so in accordance with rr 15.5 and 15.9 of the Rules.

1508. By reason of the matters pleaded at paragraph 1507, Crown Melbourne contravened s36(1) of the Act on and from 1 March 2016 with respect to Customer 33.

Particulars

Section 36(1) of the Act is a civil penalty provision: s36(2) of the Act.

Customer 34

1509. Customer 34 has been a customer of Crown Melbourne from October 2005 to May 2021.

1510. From at least December 2006 to May 2021, Crown Melbourne provided Customer 34 with designated services within the meaning of table 1 and table 3, s6 of the Act.

Particulars

On 16 May 2007, Crown Melbourne opened a DAB account and safekeeping account (AUD) for Customer 34.

On 23 October 2008, Crown Melbourne approved a credit facility (AUD) for Customer 34 of $75,000. On 22 October 2014, this credit facility was increased to $200,000. The credit facility was closed on 20 June 2021.

On 25 May 2021, Crown Melbourne issued an indefinite WOL in respect of Customer 34.

Between 2005 and 2015, Crown Melbourne recorded Customer 34's cumulative individual rated gaming activity to be buy-in of $101,981,415 with a loss of $5,845,805.

Between 2016 and 2020, Crown Melbourne recorded Customer 34's cumulative individual rated gaming activity to be buy-in of $126,911,040 with a loss of $12,799,487.

Customer 34's average bet at Crown Melbourne increased from $3,283 in 2007 to $19,858 in 2019.

1511. From at least June 2008 to 2019, Customer 34 received designated services as a junket player, facilitated through three different junket operators.

Particulars

Customer 34 was a key player in the Customer 9, and two other junket program. Between June 2008 and December 2019, Customer 34 attended 16 junket programs.

Between 2008 and 2014, Crown Melbourne recorded Customer 34's cumulative junket turnover to be $45,773,450 with a loss of $1,918,770.

In 2019, Crown Melbourne recorded Customer 34's cumulative junket turnover to be $8,440,000 with a win of $457,190.

The ML/TF risks posed by Customer 34

1512. By 1 March 2016, higher ML/TF risks were indicated by the nature and purpose of Customer 34's business relationship with Crown Melbourne, the nature of the transactions he had been conducting, together with the suspicions Crown Melbourne itself had formed with respect to Customer 34.

Particulars

Section 36(1)(a), (b) of the Act and Chapter 15 of the Rules.

Customer 34 was a junket player. He received designated services through the channel of junket programs. This channel lacked transparency: see paragraph 477.

SMRs by 1 March 2016

By 1 March 2016, Crown Melbourne had given the AUSTRAC CEO 17 SMRs in relation to Customer 34 – on 17 May 2007, 26 September 2008, 13 November 2008, 16 March 2009, 18 March 2009, 4 June 2009, 31 March 2010, 19 August 2010, 25 May 2011, 27 May 2011, 16 May 2013, 21 May 2013, 10 March 2015, 27 May 2015, 21 August 2015, 25 November 2015 and 20 January 2016. The SMRs reported Customer 34's individual and junket wins/losses, telegraphic transfers received from money changers, telegraphic transfers to a third party, large cash transactions and foreign currency exchanges and the amount of cash Customer 34 was prepared to carry.

Gaming activity by 1 March 2016

Between 2005 and 2015, Crown Melbourne recorded Customer 34's cumulative individual rated gaming activity to be buy-in of $101,981,415 with a loss of $5,845,805.

Between 2008 and 2014, Crown Melbourne recorded Customer 34's cumulative junket turnover to be $45,773,450 with a loss of $1,918,770.

Third party transactions by 1 March 2016

Between 29 May 2014 and 5 January 2016, Crown Melbourne received 23 third party transfers in a foreign currency totalling $5,909,561 from a money changer. The funds were used by Customer 34 as front money, deposited into Customer 34's DAB account or used to redeem Customer 34's credit line. However, the transactions were not identified for their high ML risk until a lookback in 2021: SMR dated 19 July 2021.

In 2021, an independent auditor identified a subset of these transactions as indicative of the ML/TF typology of cuckoo smurfing: 17 deposits totalling $4,041,576 which comprised in 88 transactions through the Southbank accounts.

On 6 March 2015, Customer 34 sent a telegraphic transfer of $700,000 to a third party.

Other large and unusual transactions by 1 March 2016

In November 2008, Crown Melbourne issued a cheque to Customer 34 for $75,000. The debt to Crown Melbourne was outstanding until March 2009, when Customer 34 repaid the debt in order to join a junket program.

Customer 34's credit line of $75,000 was cancelled due to the late repayment of the balance. On 22 October 2014, this credit facility was increased to $200,000.

Between 22 May 2015 and 27 May 2015, Customer 34 engaged in 19 cash transactions totalling $639,475 which comprised:

- four account deposits totalling $330,000;
- one buy-in totalling $10,000;
- 13 chip cash ins totalling $254,475; and
- one cash withdrawal of $45,000.

Law enforcement inquiry in 2016

On 3 February 2016, Crown Melbourne received a law enforcement inquiry in respect of Customer 34.

Due diligence conducted by 1 March 2016

By 1 March 2016, the due diligence steps taken with respect to Customer 34 included company searches for the purpose of approving Customer 34's credit facility and risk intelligence searches which returned no results.

Transactions indicative of ML/TF typologies by 1 March 2016

In 2020 and 2021, independent auditors identified the following suspicious transactions involving Customer 34:

In 2015, Customer 34 engaged in large and unusual transactions at Crown Melbourne, including:

- on 2 July 2015, Customer 34 deposited $7,703 by cash, then deposited a further $8,000 by cash on the same day; and
- on 4 November 2015, Customer 34 deposited $477 in cash, then deposited a further $6,000, $6,000 and $9,000 on 6 November 2015, and a further $400 on 10 November 2015.
- on 6 November 2015, Customer 34 deposited $6,000, $6,000 and $9,000 in cash and a further $400 on 10 November 2015.

Between 14 September 2014 and 2 January 2016, Customer 34 engaged in transactions indicative of ML/TF typologies involving smurfing, cuckoo smurfing, structuring and transfers by a money changer at Crown Melbourne.

1513. As at 1 March 2016, Customer 34 should have been recognised by Crown Melbourne as a high risk customer for the reasons pleaded at paragraph 1512.

Particulars

Section 36(1)(a), (b) of the Act and Chapter 15 of the Rules.

1514. It was not until 22 March 2021 that Customer 34 was rated high risk by Crown Melbourne.

Particulars

On various occasions between 17 May 2007 and 2 February 2016, Customer 34 was assessed by Crown Melbourne to be moderate risk.

On various occasions between 3 February 2016, after receiving a law enforcement inquiry, and 9 July 2018, Customer 34 was assessed by Crown Melbourne as significant risk.

On various occasions between 10 July 2018 and 21 March 2021, Customer 34 was assessed by Crown Melbourne to be moderate risk.

It was not until 22 March 2021 that Crown Melbourne assessed Customer 34 to be high risk. Customer 34 was assessed by Crown Melbourne to be high risk on various occasions between 22 March 2021 and 19 July 2021.

By 1 March 2016, Customer 34 had been the subject of 17 SMRs, engaged in gaming activity with a cumulative buy-in of over $100,000,000 and junket turnover of over $45,000,000, been the subject of a law enforcement inquiry and engaged in transactions indicative of the ML/TF typology of structuring, smurfing and cuckoo smurfing.

See paragraph 481.

1515. At all times on and from 1 March 2016, Customer 34 should have been recognised by Crown Melbourne as a high risk customer for the reasons pleaded at paragraphs 1512, 1516, 1517, 1518, 1519 and 1521.

Particulars

Section 36(1)(a), (b) of the Act and Chapter 15 of the Rules.

1516. On and from 1 March 2016 designated services provided to Customer 34 posed higher ML/TF risks including because the provision of designated services to Customer 34 involved a combination of the following factors:

a. Customer 34 received high value financial (table 1, s6) and gaming services (table 3, s6) provided through multiple junket programs: see paragraph 473ff;

b. Customer 34 was a junket player;

c. by 2020, Customer 34 had an individual cumulative buy-in of $228,892,455 with a loss of $18,645,292;

d. by 2019, Customer 34 had a junket cumulative turnover of $54,213,450 with a loss of $1,461,580;

e. designated services provided to Customer 34 lacked transparency as the services were provided through the channel of junket programs: see paragraph 477(e);

f. Customer 34, and persons associated with Customer 34, transacted using large amounts of cash and cash that appeared suspicious, including large volumes of cash in small notes in a suitcase: see paragraphs 450, 451, 452 and 491;

g. designated services provided to Customer 34 involved large transfers to and from third parties, including to and from foreign banks, foreign money changers and unknown third parties who were not active at Crown Melbourne: see paragraph 456ff;

h. designated services provided to Customer 34 involved large cross-border movements of funds, including through a Southbank account: see paragraph 239;

i. large values were transferred to and from Customer 34's bank accounts and his DAB account, and to and from other customers' DAB accounts, involving the provision by Crown Melbourne of designated services within the meaning of items 31 and 32, table 1, s6 of the Act: see paragraphs 411ff and 492;

j. at various times, Customer 34 was provided with significant amounts of credit upon request, up to limits of $200,000: see paragraph 280ff;

k. Customer 34 engaged in other transactions indicative of ML/TF typologies and vulnerabilities, including structuring, smurfing and cuckoo smurfing: see paragraph 24;

l. these transactions took place against the background of:

   i. law enforcement having expressed an interest in Customer 34 in 2016;

   ii. sums deposited by a money changer originated in 88 transactions the majority of which comprised small cash deposits at various bank branches;

   iii. 17 SMRs being given to the AUSTRAC CEO by Crown Melbourne by 1 March 2016;

m. in March 2021, Customer 34 refused to provide evidence of his source of wealth; and

n. by reason of the matters set out at subparagraphs a. to m. above, there were real risks that Customer 34's source of wealth and source of funds were not legitimate.

Monitoring of Customer 34's transactions

1517. At no time did Crown Melbourne appropriately monitor Customer 34's transactions on a risk-basis.

Particulars

Section 36(1)(a), (b) of the Act and rules 15.4 to 15.8 of the Rules.

Crown Melbourne was unable to monitor the ML/TF risks posed by Customer 34's transactions appropriately because it did not make and keep appropriate records of designated services provided to junket players: see paragraphs 483ff.

Crown Melbourne did not apply appropriate risk-based transaction monitoring to designated services provided to Customer 34: see paragraphs 590ff, 629 to 642 and 643 to 649.

Customer 34's transactions involved repeated transactions indicative of ML/TF typologies and vulnerabilities that were not detected prior to a 2021 lookback. Had appropriate risk-based transaction monitoring been applied, these transactions could have been identified earlier: see paragraphs 686 and 687.

In addition to the transactions at paragraph 1518, between 24 March 2016 and 27 June 2016, Customer 34 received deposits from a

money changer totalling $1,042,624 indicative of the ML/TF typology of cuckoo smurfing:

- $93,897 comprised of a telegraphic transfer from a money changer (Company 3) of $93,897 on 24 March 2016;
- $331,126 comprised of five telegraphic transfers from a money changer (Company 3) ranging between $56,000 and $77,500 on 19 May 2016 and 20 May 2016;
- $198,020 comprised of six telegraphic transfers from a money changer (Company 3) ranging from $55,000 to $78,020 on 23 May 2016 and 25 May 2016;
- $227,273 comprised of three telegraphic transfers from a money changer (Company 3) ranging from $71,573 to $78,200 on 8 June 2016; and
- $192,308 comprised of two telegraphic transfers from a money changer (Company 3) ranging from $95,980 to $96,328.

Ongoing customer due diligence

1518. On and from 1 March 2016, on multiple occasions, the provision of designated services to Customer 34 raised red flags reflective of higher ML/TF risks as a result of Customer 34's frequent, large transactions with a number of third parties.

Particulars

See paragraph 456ff.

Large and suspicious transactions in 2017

On 27 July 2017, Customer 34 received a telegraphic transfer of $9,025 from a third party: SMR dated 30 August 2017.

On 28 July 2017, Customer 34 received a telegraphic transfer of $20,000 from a third party: SMR dated 30 August 2017.

On 29 August 2017, another Crown Melbourne patron transferred $85,000 to Customer 34's DAB account. The other Crown Melbourne patron had deposited the funds into their DAB account in cash: SMR dated 29 August 2017.

On 29 August 2017, Customer 34 received a telegraphic transfer of $6,000 from a third party: SMR dated 30 August 2017.

On 27 September 2017, a third party transferred $42,000 to Customer 34's DAB account. The third party had no history at Crown Melbourne and presented the funds in cash: SMR dated 27 September 2017.

Large and suspicious transactions in 2018

On 15 February 2018, Customer 34 received two telegraphic transfers from a foreign bank totalling $205,625 and three telegraphic

transfers from a second foreign bank totalling $277,000: SMR dated 16 February 2018.

On 17 February 2018, another Crown Melbourne patron transferred $300,000 to Customer 34's DAB account. Customer 34 withdrew the funds on the same day. The other patron had deposited a total of $590,090 in cash, withdrawn $290,090 in cash and transferred the balance to Customer 34: SMR dated 28 February 2018.

On the same day, Customer 34 received $1,000,000 from Person 33. Person 33 had presented at the Crown Melbourne Cage with a suitcase containing $1,300,000 in cash comprised mostly of $50 notes. He had no account at Crown and claimed to be a tourist. Person 33 claimed that the money came from an Australian bank withdrawn over several days from one bank branch: SMR dated 5 March 2018.

On 5 March 2018, another Crown Melbourne patron transferred $1,000,000 to Customer 34's DAB account.

Large and suspicious transactions in 2019

On 4 June 2019, Customer 34 transferred $500,000 to the DAB account of another Crown Melbourne patron, Person 33. Crown Melbourne then arranged for a telegraphic transfer to be sent from this Crown Melbourne patron to the personal account of a second Crown Melbourne patron. On 5 June 2019, Customer 34 sent a telegraphic transfer of $450,000 to the personal account of the second Crown Melbourne patron: SMR dated 6 June 2019.

On 22 July 2019, Customer 34 received a telegraphic transfer of $20,000 from a third party: SMR dated 23 July 2019.

1519. On and from 1 March 2016, on multiple occasions, the provision of designated services to Customer 34 raised red flags reflective of higher ML/TF risks as a result of complex, unusual large transactions and unusual patterns of transactions involving Customer 34 which had no apparent economic or visible lawful purpose.

Particulars

See paragraphs 450 and 451.

Unusual transactions and patterns of transactions in 2016

In 2016, Customer 34 had a cumulative buy-in of $20,328,950 with a loss of $5,737,315.

Between 25 June 2016 and 26 June 2016, Customer 34 made four chip cash ins totalling $67,418 and a cash withdrawal of $10,000.

On 27 June 2016, Customer 34 made an account deposit of $30,000.

Unusual transactions and patterns of transactions in 2017

In 2017, Customer 34 had a cumulative buy-in of $25,646,635 with a loss of $3,619,682.

Between 8 April 2017 and 9 April 2017, Customer 34 made a chip cash in of $10,000 and an account deposit of $30,000.

On 10 April 2017, Customer 34 made an account deposit of $20,000.

On 11 April 2017, Customer 34 made two chip cash ins totalling $28,400 and a cash withdrawal of $16,215.

On 27 July 2017, Customer 34 made a chip cash in of $45,000 and a cash withdrawal of $22,750.

Between 28 July 2017 and 29 July 2017, Customer 34 made five account deposits totalling $395,001.

Unusual transactions and patterns of transactions in 2018

In 2018, Customer 34 had a cumulative buy-in of $17,492,920 with a loss of $2,235,635.

On 30 August 2018, Customer 34 made two cash withdrawals totalling $26,460.

On 15 February 2018, Customer 34 made an account deposit of $400,000. The cash comprised $50 notes with no straps or other markings. Customer 34 also received six telegraphic transfers totalling $602,625. On the following day, Customer 34 deposited a further $350,000 in cash: SMR dated 16 February 2018.

On 27 February 2018, Customer 34 made a cash withdrawal of $290,000.

On 2 March 2018, Customer 34 sent a telegraphic transfer of $482,625 to a Southbank account.

Unusual transactions and patterns of transactions in 2019

For 2019, Customer 34 had a cumulative buy-in of $63,442,535 with a loss of $1,207,125.

In 2019, Crown Melbourne recorded Customer 34's cumulative junket turnover to be $8,440,000 with a win of $457,190.

On the following occasions, Customer 34 attended a junket program:

- 10 October 2019 to 17 October 2019. Customer 34 had a turnover of $5,400,000 with a win of $857,750;
- 21 October 2019 to 10 November 2019. Customer 34 had a turnover of $1,140,000 with a loss of $200,000; and
- 12 November 2019 to 12 December 2019. Customer 34 had a turnover of $1,900,000 with a loss of $200,000.

On 11 March 2019, Customer 34 made a cash withdrawal of $230,300, a chip cash in of $10,000 and two account deposits totalling $200,000. Customer 34 had presented with $830,300 in gaming chips, deposited the chips into his account and withdrew $230,300: SMR dated 12 March 2019.

1520. At no time did Crown Melbourne undertake appropriate risk-based customer due diligence with respect to Customer 34 with a view to identifying, mitigating and managing the ML/TF risks posed by the provision of designated services on and from 1 March 2016.

a. It was not until 2021 that Crown Melbourne took appropriate steps to determine whether Customer 34's source of wealth/funds was legitimate.

b. It was not until 2021 that Crown Melbourne took appropriate steps to identify or analyse the ML/TF risks of Customer 34's transactions or to consider whether they had a lawful purpose.

c. Crown Melbourne gave no consideration at any time to whether large and high risk transactions should be processed. In 2021, over five years after then were processed, Crown Melbourne considered the suspicious transactions which occurred in 2015 – 2016.

d. On each occasion prior to May 2021 that senior management considered whether to continue the business relationship with Customer 34, senior management failed to give adequate consideration to whether the ML/TF risks posed by Customer 34 were within Crown Melbourne's risk appetite.

Particulars

Section 36(1)(a) of the Act.

The due diligence steps taken with respect to Customer 34 included:

Wealth and risk intelligence reports

In January 2019 and January 2021, Crown Melbourne obtained a wealth report in respect of Customer 34. The January 2021 wealth report identified Customer 34's wealth band to be between very high.

In January 2021, Crown Melbourne obtained a risk intelligence report in respect of Customer 34. The report estimated Customer 34's high net worth based on shareholdings and company information, and noted that Customer 34 was affiliated with a foreign PEP through common shareholdings.

Due diligence searches

Between May 2016 and December 2020, Crown Melbourne conducted company searches, risk intelligence searches, DJRC searches, land registry searches, and open source media searches in respect of Customer 34.

Senior management engagement

In March 2019 and October 2020, the CTRM updated Customer 34's profile.

In November 2020, Crown Melbourne prepared a KYC profile in respect of Customer 34. The profile noted that Customer 34 had participated in extensive third-party transactions and suspicious cash deposits and had been involved in play period violations and breaches. The profile included a recommendation that further AML

and compliance scrutiny be taken in respect of Customer 34 and that he be referred to the POI Committee.

On 18 November 2020, the POI Committee determined that it would seek source of wealth information in respect of Customer 34. In January 2021, Crown Melbourne obtained a wealth and risk intelligence report, which identified Customer 34's estimated wealth.

By 13 January 2021, Crown Melbourne had prohibited Customer 34 from attending the property until a Source of Wealth statement had been lodged. The Group Senior Manager (AML – Customer Intelligence & Due Diligence) noted AML concerns as a factor which led to a POI decision about Customer 34 pending the provision of a Source of Wealth statement.

In January 2021, Crown Melbourne prepared a debtor due diligence profile for the purpose of assessing Customer 34's creditworthiness.

On 20 January 2021, the POI Committee decided to wait until Customer 34's source of wealth information had been obtained to determine whether or not to issue him with a WOL, and noted that Customer 34 had been overseas and so had not provided this information.

On 22 March 2021, Customer 34 refused to provide evidence of his source of wealth.

On 25 May 2021, Crown Melbourne issued Customer 34 with a WOL.

Until May 2021, none of these steps were proportionate to the ML/TF risks reasonably posed by Customer 34 on and from 1 March 2016.

Enhanced customer due diligence

1521. Having formed a suspicion for the purposes of s41 of the Act, Crown Melbourne gave the AUSTRAC CEO SMRs with respect to Customer 34 on:

a. 28 June 2016;

b. 11 April 2017;

c. 29 August 2017;

d. 30 August 2017;

e. 27 September 2017;

f. 16 February 2018;

g. 28 February 2018;

h. 5 March 2018;

i. 12 March 2019;

j. 6 June 2019;

k. 23 July 2019;

l. 17 November 2020;

m. 3 June 2021; and

n. 19 July 2021.

Particulars

Prior to the 17 November 2020 SMR, the SMRs described Customer 34's annual losses, third party and company transfers including transfers from third party with no associated gaming activity, large cash transactions and the amount of cash Customer 34 was prepared to carry.

The 17 November 2020, 3 June 2021 and 19 July 2021 SMRs reported transactions identified in the look back: see particulars to paragraph 1512.

1522. On each occasion that Crown Melbourne formed a suspicion with respect to Customer 34 for the purposes of s41 of the Act, it was required to apply its ECDD program to Customer 34.

Particulars

Rule 15.9(3) of the Rules.

1523. Crown Melbourne did not carry out appropriate risk-based ECDD measures with respect to Customer 34 on each occasion that Crown Melbourne formed a suspicion with respect to Customer 34 for the purposes of s41 of the Act.

a. With the exception of the 16 February 2018 and 17 November 2020 SMRs, there are no records of ECDD being conducted following the lodgement of any SMRs: see paragraphs 664, 666 and 685.

b. Until 2021, appropriate risk-based steps were not taken to obtain or analyse information about Customer 34's source of wealth/funds: see paragraph 667.

c. Appropriate risk-based steps were not taken to analyse and monitor Customer 34's transactions – both past and future – including to understand their economic purpose: see paragraph 590 and 666.

d. On each occasion prior to May 2021 that senior management considered whether to continue the business relationship with Customer 34, senior management failed to give adequate consideration to whether the ML/TF risks posed by Customer 34 were within Crown Melbourne's risk appetite.

Particulars

Rules 15.9(3), 15.10(1)(c), (d), (2), (5) and (6) of the Rules.

After lodging an SMR on 16 February 2018, Crown Melbourne conducted risk intelligence searches and company searches in respect of Customer 34 which did not reveal any new information. However, Crown Melbourne did not take appropriate steps to identify Customer 34's source of wealth/funds or to determine whether that source was legitimate.

Prior to and following the lodgement of the SMR on 17 November 2020, Crown Melbourne appears to have conducted various searches in respect to Customer 34. However, these searches simply confirmed that Crown Melbourne had no records to substantiate

Customer 34's source of wealth/funds. It was not until March 2021 that Customer 34 ultimately refused to provide evidence of his source of wealth.

1524. By reason of the matters pleaded from paragraphs 1509 to 1523, on and from 1 March 2016, Crown Melbourne:

a. did not monitor Customer 34 in relation to the provision of designated services, with a view to identifying, mitigating and managing the ML/TF risks it reasonably faced; and

b. did not do so in accordance with rr 15.5 and 15.9 of the Rules.

1525. By reason of the matters pleaded at paragraph 1524, Crown Melbourne contravened s36(1) of the Act on and from 1 March 2016 to 25 May 2021 with respect to Customer 34.

Particulars

Section 36(1) of the Act is a civil penalty provision: s36(2) of the Act.

Customer 35

1526. Customer 35 has been a customer of Crown Melbourne since 28 October 1999.

1527. From at least December 2006 to 18 September 2021, Crown Melbourne provided Customer 35 with designated services within the meaning of table 3, s6 of the Act.

1528. From at least December 2006 to 18 September 2021, Customer 35 received designated services within the meaning of table 3, s6 of the Act as a junket player, facilitated through six different junket operators.

Particulars to paragraphs 1527 and 1528

Customer 35 received designated services through the Suncity junkets and five other junkets.

Between 5 March 2004 and 23 December 2007, Customer 35 attended five junket programs with a cumulative turnover of $121,000,000 and loss of $5,515,150.

Between 1 June 2016 and 30 September 2019, Customer 35 attended five junket programs with a cumulative turnover of $106,843,864 and loss of $2,892,527.

The ML/TF risks posed by Customer 35

1529. By 1 March 2016, higher ML/TF risks were indicated by the nature and purpose of Customer 35's business relationship with Crown Melbourne, the nature of the transactions he had been conducting, together with the suspicions Crown Melbourne itself had formed with respect to Customer 35.

Particulars

Section 36(1)(a), (b) of the Act and Chapter 15 of the Rules.

Customer 35 was a junket player. He received designated services through the channel of junket programs. This channel lacked transparency: see paragraph 477.

By 1 March 2016, Crown Melbourne had not given the AUSTRAC CEO any SMRs in respect of Customer 35 despite his cumulative turnover of $121,000,000 and actual loss of $5,515,150 across five junket programs.

1530. At all times on and from 1 March 2016, Customer 35 was rated as high risk by Crown Melbourne.

Particulars

On various occasions after 26 June 2014, Crown Melbourne rated Customer 35's risk as high.

On 3 May 2010, Crown Melbourne first identified Customer 35 to be a foreign PEP as a result of a risk intelligence search. Crown Melbourne rated Customer 35's risk as significant.

On 26 June 2014, Crown Melbourne conducted a risk intelligence search which again determined Customer 35 to be a foreign PEP. Crown Melbourne rated Customer 35's risk as high for the first time.

On 22 July 2014, the Executive General Manager (Legal and Regulatory Services) approved a continuing business relationship with Customer 35.

See paragraph 481.

1531. On and from 1 March 2016 designated services provided to Customer 35 posed higher ML/TF risks including because the provision of designated services to Customer 35 involved a combination of the following factors:

a. Customer 35 was a foreign PEP: see paragraphs 118 and 663;

b. Customer 35 was a junket player;

c. Customer 35 received high value gaming services (table 3, s6) provided through multiple junket programs including the Suncity junket;

d. designated services provided to Customer 35 lacked transparency as the services were provided through the channel of junket programs: see paragraph 477(e);

e. between June 2016 and September 2019, Customer 35's junket turnover exceeded $106,000,000 with a loss of $2,892,527;

f. the table 3, s6, designated services provided to Customer 35 involved high turnover.

g. Customer 35 operated a casino in a foreign country;

h. in March 2016, media articles reported that a close relative of Customer 35's operated an illicit international gambling ring with an estimated turnover of $1,750,000,000 for which Customer 35's relative was sentenced to ten years' imprisonment, and that the relative was at large in a foreign country;

i. by March 2019, Crown Melbourne was aware of media articles which reported that Customer 35 had strong ties to the governing party in a foreign country. By June 2021, Crown Melbourne was aware of media articles which reported that that a number of individuals had been arrested at a casino operated by Customer 35; and

j. by reason of the matters set out at subparagraphs a. to i. above, there were higher ML/TF risks associated with Customer 35's source of wealth/funds

Monitoring of Customer 35's transactions

1532. At no time did Crown Melbourne appropriately monitor Customer 35's transactions on a risk-basis.

Particulars

Section 36(1)(a), (b) of the Act and rules 15.4 to 15.8 of the Rules.

Crown Melbourne was unable appropriately to monitor the ML/TF risks posed by Customer 35's transactions because it did not make and keep appropriate records of designated services provided to junket players: see paragraphs 483ff.

Crown Melbourne did not apply appropriate risk-based transaction monitoring to designated services provided to Customer 35: see paragraphs 590ff, 629 to 642 and 643 to 649.

Ongoing customer due diligence

1533. On and from 1 March 2016, on multiple occasions, the provision of designated services to Customer 35 raised red flags reflective of higher ML/TF risks as a result of Customer 35's recorded individual and junket play which involved high turnover.

Particulars

See paragraph 477.

Between 1 June 2016 and 30 June 2016, Customer 35 was a key player on a Suncity junket program and had an estimated turnover of $14,930,000 and an estimated win of $146,700.

Between 26 August 2017 and 26 September 2017, Customer 35 was a key player in a junket program and had an estimated turnover of $3,140,000 and an estimated win of $287,300.

Between 5 September 2018 and 17 September 2018, Customer 35 was a key player in a junket program and had an estimated turnover of $3,075,980 and estimated win of $149,658.

Between 9 March 2019 and 20 March 2019, Customer 35 was a key player in a junket program and had an estimated turnover of $45,718,447 and estimated actual loss of $1,135,500.

By 20 March 2019, Customer 35's junket losses in 2019 was HKD6,300,000 (AU$1,130,000) and he had no individual rated gaming activity. Crown Melbourne rated Customer 35's risk as high: SMR dated 20 March 2019.

Between 1 September 2019 and 30 September 2019, Customer 35 was a key player on a Suncity junket program and had an estimated turnover of $39,979,437 and an estimated loss of $2,340,685.

By 1 October 2019, Customer 35's junket losses in 2019 had increased to $2,282,040 and he had no individual rated gaming activity: SMR dated 1 October 2019.

On 27 November 2019, Crown Melbourne last provided a designated service to Customer 35.

By 18 September 2021, Crown Melbourne had put stop codes in place in respect of Customer 35.

1534. Between at least February 2006 and June 2021 a number of widely accessible media reports were published in respect of Customer 35. These articles do not appear to have come to Crown Melbourne's attention as part of its due diligence process.

Particulars

The articles reported:

- Customer 35's political career and business history; and
- that Customer 35's close relative had been sentenced to 10 years' imprisonment in 2013 for masterminding an illicit international gambling ring in a foreign country with an estimated turnover of $1,750,000,000.

1535. At no time did Crown Melbourne undertake appropriate risk-based customer due diligence with respect to Customer 35 with a view to identifying, mitigating and managing the ML/TF risks posed by the provision of designated services on and from 1 March 2016.

a. At no time did Crown Melbourne take appropriate steps to understand whether Customer 35's source of wealth/funds was legitimate.

b. At no time did Crown Melbourne take appropriate steps to identify or analyse the ML/TF risks of Customer 35's transactions or to consider whether they had a lawful purpose.

c. On each occasion that senior management considered whether to continue the business relationship with Customer 35, senior management failed to give adequate consideration to whether the ML/TF risks posed by Customer 35 were within Crown Melbourne's risk appetite.

Particulars

Section 36(1)(a) of the Act.

The due diligence steps taken with respect to Customer 35 included:

Database searches

Crown Melbourne conducted risk intelligence searches in December 2018 and March 2019.

Crown Melbourne conducted open source media searches in March 2019. These searches identified Customer 35 as the operator of a casino in a foreign country and a director of the company that owned that casino.

Crown Melbourne obtained a wealth report in respect of Customer 35 in May 2019 and June 2019. The May 2019 report stated that Customer 35 and a high estimated net worth.

In June 2021, Crown conducted searches in respect of Customer 35 and his company which identified a number of media articles published between January 2012 and March 2016.

Senior management consideration

On 7 March 2019, the Group General Manager (AML) requested copies of Crown Melbourne's due diligence for Customer 35. She was sent a copy of the March 2019 risk intelligence searches. She was also advised that a wealth report had been ordered. However, the report was not downloaded until two months later.

In March 2019, the CTRM reviewed Crown Melbourne's customer information relating to Customer 35.

On 20 March 2019, the Group General Manager (AML) sent an email to the CTRM identifying Customer 35's junket turnover and estimated loss.

In October 2019, the CTRM reviewed a number of key players in junket programs who had lost more than $90,000, including Customer 35.

On 17 March 2020, the AML Manager confirmed that Customer 35 had been approved as part of a bulk approval process in July 2014.

None of these steps were proportionate to the ML/TF risks reasonably posed by Customer 35 on and from 1 March 2016.

By 18 September 2021, stop codes were in place in respect of Customer 35.

Enhanced customer due diligence

1536. Having formed a suspicion for the purposes of s41 of the Act, Crown Melbourne gave the AUSTRAC CEO SMRs with respect to Customer 35 on:

a. 20 March 2019; and

b. 1 October 2019.

Particulars

Each of these SMRs reported high junket losses experienced by Customer 35.

1537. On each occasion that Crown Melbourne formed a suspicion with respect to Customer 35 for the purposes of s41 of the Act, it was required to apply its ECDD program to Customer 35.

Particulars

Rule 15.9(3) of the Rules.

1538. Crown Melbourne did not carry out appropriate risk-based ECDD measures with respect to Customer 35 on each occasion that Crown Melbourne formed a suspicion with respect to Customer 35 for the purposes of s41 of the Act.

a. There are no records of ECDD being conducted following the lodgement of either SMR: see paragraphs 664 and 685.

b. Appropriate risk-based steps were not taken to obtain or analyse information to determine the legitimacy of Customer 35's source of wealth/funds: see paragraph 667.

c. On each occasion that senior management considered whether to continue the business relationship with Customer 35, senior management failed to give adequate consideration to whether the ML/TF risks posed by Customer 35 were within Crown Melbourne's risk appetite.

Particulars

Rules 15.9(3), 15.10(1)(c), (d), (2), (5) and (6) of the Rules.

1539. At all times from 1 March 2016, Customer 35 was a foreign PEP.

Particulars

Section 36(1)(a) of the Act.

On 3 May 2010, Crown Melbourne first identified Customer 35 to be a foreign PEP as a result of a risk intelligence search. Customer 35 was a member in a foreign government: see particulars to paragraph 1530.

1540. At all times from 1 March 2016, Crown Melbourne was required to apply its ECDD program to Customer 35.

Particulars

Rules 15.9(2), 15.11 of the Rules

See paragraphs 660, 663 and 666.

1541. Crown Melbourne did not carry out appropriate risk-based ECDD measures with respect to Customer 35 on and from 1 March 2016 given his status as a foreign PEP. In particular:

a. Crown Melbourne did not undertake a detailed analysis of Customer 35's KYC information or analyse the legitimacy of Customer 35's source of wealth/funds;

b. on occasions where senior management approved a continuing business relationship with Customer 35 as a foreign PEP prior to 1 March 2016, the decision did not have adequate regard to the ML/TF risks posed by Customer 35 given his status as a foreign PEP because it was part of a bulk approval process; and

c. on occasions where senior management approved continuing to provide designated services to Customer 35 as a foreign PEP prior to 1 March 2016, the decision did not have adequate regard to the ML/TF risks posed by Customer 35 given his status as a foreign PEP because it was part of a bulk approval process.

Particulars

Rules 15.10(2), 15.10(6), 15.11 of the Rules.

See paragraphs 1535 and 1538.

See paragraph 660, 663, 666, 667 and 668.

1542. On and from 1 March 2016, Crown Melbourne rated Customer 35 high risk.

Particulars

Crown Melbourne rated Customer 35 high risk on six occasions after 18 September 2018: see paragraph 1530.

1543. On each occasion that Crown Melbourne rated Customer 35 high risk, Crown Melbourne was required to apply its ECDD program to Customer 35.

Particulars

Rule 15.9(1) of the Rules.

See paragraph 661.

1544. Crown Melbourne did not carry out appropriate risk-based ECDD measures with respect to Customer 35 on each occasion that Crown Melbourne rated Customer 35 high risk.

Particulars

There is no record of ECDD being conducted following each occasion that Crown Melbourne rated Customer 35 high risk.

See paragraphs 1535 and 1538.

See paragraphs 661, 666, 667 and 668.

1545. By reason of the matters pleaded from paragraphs 1526 to 1544, on and from 1 March 2016, Crown Melbourne:

a. did not monitor Customer 35 in relation to the provision of designated services, with a view to identifying, mitigating and managing the ML/TF risks it reasonably faced; and

b. did not do so in accordance with rr 15.5 and 15.9 of the Rules.

1546. By reason of the matters pleaded at paragraph 1545, Crown Melbourne contravened s36(1) of the Act on and from 1 March 2016 with respect to Customer 35.

Particulars

Section 36(1) of the Act is a civil penalty provision: s36(2) of the Act.

Customer 36

1547. Customer 36 was a customer of Crown Melbourne from September 1996 to June 2021.

1548. From at least December 2006 to June 2021, Crown Melbourne provided Customer 36 with designated services within the meaning of table 1 and table 3, s6 of the Act.

1549. From at least August 2010 to June 2021, Customer 36 received designated services as a junket operator and junket player at Crown Melbourne.

Particulars to paragraphs 1548 and 1549

On 25 May 2017 and 28 October 2019, Crown Melbourne entered into a NONEGPRA with Customer 36 to operate junkets at Crown Melbourne.

On various occasions, Customer 36 was a key player in his own junket. Customer 36 was also a junket representative for another junket program.

On 22 September 1996, Crown Melbourne opened a DAB account and a safekeeping account (AUD/HKD) for Customer 36, which were closed on 12 November 2021. On 12 March 2019, Crown Melbourne opened a further DAB account and safekeeping account (AUD) for Customer 36, which were closed on 12 November 2021.

On 18 February 2009, Crown Melbourne approved a credit facility (AUD/HKD) for Customer 36 which was closed on 23 November 2020.

On 22 June 2021, Crown Melbourne issued an indefinite WOL in respect of Customer 36.

By July 2019, Crown Melbourne recorded Customer 36's individual rated gaming activity to be a cumulative buy-in of $72,452,134 with a cumulative loss of $6,144,495.

By December 2019, Crown Melbourne recorded Customer 36's individual gaming activity and gaming activity on junket programs run by Customer 36 as a cumulative turnover of $663,935,837 with a cumulative loss of $6,101,570.

1550. Customer 36 has been a customer of Crown Perth from February 1996 to June 2021.

1551. From at least December 2006 to June 2021, Crown Perth provided Customer 36 with designated services within the meaning of table 1 and table 3, s6 of the Act.

1552. From at least December 2006 to June 2021, Customer 36 received designated services as a junket operator and junket player at Crown Perth.

Particulars to paragraphs 1551 and 1552

On 28 August 2003 and 28 October 2019, Crown Perth entered into a NONEGPRA with Customer 36 to operate junkets at Crown Perth. In 2018 and 2019, Customer 36 operated four junket programs.

On various occasions, Customer 36 was a key player in his own junket. Customer 36 was also a junket representative for another junket operator.

On 28 February 1996, Crown Perth opened a DAB account and safekeeping account (AUD/HKD) for Customer 36, both of which remain open. On 20 March 2008 and 3 November 2018, Crown Perth opened two further DAB accounts and safekeeping accounts (AUD/HKD) for Customer 36 under different PIDs.

On 19 April 2011, Crown Perth approved a credit facility (AUD/HKD) for Customer 36 of $500,000. On 2 November 2018, the credit limit was increased to $5,000,000. The credit facility was closed on 23 November 2020.

By May 2021, Crown Perth recorded Customer 36's individual gaming activity and gaming activity on junket programs run by Customer 36 as a cumulative turnover of $105,595,037 with a cumulative win of $3,324,835.

On 22 June 2021, Crown Melbourne issued an indefinite NRL in respect of Customer 36.

The ML/TF risks posed by Customer 36

1553. By 1 March 2016, higher ML/TF risks were indicated by the nature and purpose of Customer 36's business relationship with Crown Melbourne and Crown Perth, the nature of the transactions he had been conducting, together with the suspicions Crown Melbourne itself had formed with respect to Customer 36.

Particulars

Section 36(1)(a) and (b) of the Act and Chapter 15 of the Rules.

Customer 36 was a junket operator and player. He received designated services through the channel of junket programs. This channel lacked transparency: see paragraph 477.

SMRs by 1 March 2016

By 1 March 2016, Crown Melbourne had given the AUSTRAC CEO three SMRs in relation to Customer 36 – on 30 August 2010, 17 March 2011 and 13 August 2013. The SMRs reported transfers of funds between DAB accounts, losses experienced by key players in Customer 36's junket and the amount of cash key players in Customer 36's junket were prepared to carry.

Gaming activity by 1 March 2016

Between 1995 and 2013, Crown Melbourne recorded Customer 36's individual rated gaming activity as cumulative buy-in of $7,799,350 with a loss of $819,853.

Large and suspicious transactions by 1 March 2016

On 30 August 2010, Customer 36 transferred $50,000 to a Crown Melbourne patron who had been involved in other large cash transactions: SMR dated 30 August 2010.

On 16 March 2011, a Crown Melbourne patron deposited $100,000 in cash into his DAB account and then transferred that amount to Customer 36's account. The patron was a key player under a junket program, but not Customer 36's junket program: SMR dated 17 March 2011.

Cash deposits indicative of the ML/TF typology of structuring

On 21 and 22 November 2013, $24,000 was deposited into a Riverbank account at four different branches of an Australian bank in deposits of $7,500, $5,500, $5,000 and $6,000. The deposits were indicative of the ML/TF typology of structuring.

On 25 November 2013, Crown Perth released the funds and $24,000 was placed into Customer 36's account. On 29 November 2013, Customer 36 requested that the funds be transferred to another patron. No information was known about the relationship between these customers.

The transactions were only identified as suspicious in October 2020 as a result of a lookback: SMR dated 22 October 2020.

Due diligence steps by 1 March 2016

By 1 March 2016, no due diligence steps were taken with respect to Customer 36 despite his status as a junket operator and his significant junket and individual gaming activity.

1554. On and from June 2016, Customer 36 should have been recognised by Crown Melbourne as a high risk customer for the reasons pleaded at paragraphs 1553, 1558, 1559, 1560, 1561, 1562 and 1564.

Particulars

Section 36(1)(a), (b) of the Act and Chapter 15 of the Rules.

1555. At no time was Customer 36 rated high risk by Crown Melbourne.

Particulars

On various occasions between 30 August 2010 and 5 April 2019, Crown Melbourne assessed Customer 36 to be moderate risk.

This was despite the June 2016 transactions indicative of the ML/TF typologies of structuring, smurfing and cuckoo smurfing: see paragraph 1559.

See paragraph 481.

1556. On and from June 2016, Customer 36 should have been recognised by Crown Perth as a high risk customer for the reasons pleaded at paragraph 1553, 1558, 1559, 1560, 1561, 1562 and 1565.

Particulars

Section 36(1)(a), (b) of the Act and Chapter 15 of the Rules.

1557. At no time was Customer 36 rated high risk by Crown Perth.

Particulars

On various occasions between 25 November 2013 and 26 November 2019, Crown Perth assessed Customer 36 as moderate risk.

On 27 November 2019, Crown Perth assessed Customer 36 as low risk.

This was despite the deposits at Crown Perth indicative of the ML/TF typology of structuring that took place in November 2013 through a Riverbank account: see paragraph 1553.

See paragraph 481.

1558. On and from June 2016, designated services provided to Customer 36 posed higher ML/TF risks including because the provision of designated services to Customer 36 involved a combination of the following factors:

a. Customer 36 was a junket operator;

b. Customer 36 was a junket player;

c. Customer 36 received high value financial (table 1, s6) and gaming services (table 3, s6) provided through junket programs: see paragraph 473ff;

d. Customer 36 was a junket operator who facilitated the provision of high value financial and gaming services (tables 1 and 3, s6) to multiple players on his junket programs: see paragraph 473ff;

e. by July 2019, Crown Melbourne recorded Customer 36's individual gaming activity and gaming activity on junket programs run by Customer 36 as having a cumulative turnover of $660,000,000 with a loss of $6,101,570;

f. by July 2019, Crown Perth recorded Customer 36's individual gaming activity and gaming activity on junket programs run by Customer 36 as a cumulative turnover of $105,000,000 with a win of $3,324,835;

g. by July 2019, Customer 36’s individual rated gaming activity at Crown Melbourne exceeded a cumulative buy-in of $72,000,000 with a cumulative loss of $6,144,495;

h. Customer 36 was known at all times to be connected to other junket operators, including junket operators in respect of whom Crown Melbourne had formed suspicions (including Person 20);

i. designated services provided to Customer 36 lacked transparency as the services were provided through the channel of junket programs: see paragraph 477(e);

j. Customer 36, and persons associated with his junket, transacted using large amounts of cash and cash that appeared suspicious: see paragraphs 450, 451, 452 and 491;

k. designated services provided to Customer 36 involved large transfers to and from third parties, including to and from other junket operators, foreign remittance service providers and unknown third parties: see paragraph 456ff;

l. funds transferred from Customer 36 to other junket operators included transactions related to debt settlement or offsets not related to Customer 36's junket;

m. designated services provided to Customer 36 involved large cross-border movements of funds, including through the Southbank accounts: see paragraph 239;

n. large values were transferred to and from Customer 36's bank accounts and his DAB account, and to and from other customers' DAB accounts, involving the provision by Crown Melbourne of designated services within the meaning of items 31 and 32, table 1, s6 of the Act: see paragraphs 411ff and 492;

o. at various times, Customer 36 was provided with significant amounts of credit upon request, up to limits of $5,000,000: see paragraphs 280ff and 487;

p. Customer 36 was a prominent junket operator at several foreign casinos;

q. Customer 36 made large transfers and unusual requests for transfers to overseas casinos: see paragraphs 398ff and 407ff;

r. at various times, Customer 36 had significant parked or dormant funds in his safekeeping account: see paragraph 252;

s. Customer 36 engaged in transactions indicative of ML/TF typologies and vulnerabilities, including structuring, smurfing and cuckoo smurfing through the Riverbank and Southbank accounts: see paragraph 24;

t. these transactions took place against the background of:

   i. by 1 March 2016, Customer 36 had engaged in transactions indicative of the ML/TF typology of structuring;

   ii. three SMRs being given to the AUSTRAC CEO by Crown Melbourne; and

u. by reason of the matters pleaded at paragraphs a. to t. above, there were real risks that Customer 36's source of wealth and source of funds were not legitimate.

Monitoring of Customer 36's transactions

1559. At no time did Crown Melbourne or Crown Perth appropriately monitor Customer 36's transactions on a risk-basis.

Particulars

Section 36(1)(a), (b) of the Act and Rules 15.4 to 15.8 of the Rules.

Crown Melbourne and Crown Perth were unable to monitor the ML/TF risks posed by Customer 36's transactions appropriately because they did not make and keep appropriate records of designated services provided to junket players or junket operators: see paragraph 483ff.

Crown Melbourne and Crown Perth were unable to monitor the ML/TF risks posed by transactions associated with Customer 36's junkets, including transactions by his junket representatives and key players on his junkets, because they did not make and keep

appropriate records of designated services provided to junket players, junket representatives or junket operators.

Crown Melbourne and Crown Perth did not apply appropriate risk-based transaction monitoring to designated services provided to Customer 36: see paragraphs 590ff, 629 to 649.

Customer 36's transactions involved repeated transactions indicative of ML/TF typologies and vulnerabilities that were not detected prior to a 2021 lookback. Had appropriate risk-based transaction monitoring been applied, these transactions could have been identified earlier: see paragraphs 686 and 687.

Transactions indicative of an ML/TF typology – structuring

Transactions involving Customer 36 were identified as indicative of the ML/TF typology of structuring by an independent auditor in 2021. The audit identified 90 suspicious deposits made between 9 June 2016 and 24 June 2016 totalling $710,500 at 26 bank branches in Sydney:

- on 9 June 2016, 15 deposits of $7,500 (totalling $112,500) in favour of Customer 36 at 15 different bank branches in Sydney;
- on 10 June 2016, eight deposits of $7,500 (totalling $60,000) in favour of Customer 36 at eight different bank branches in Sydney;
- on 14 June 2016, 13 deposits of $7,500 (totalling $97,500) in favour of Customer 36 at 13 different bank branches in Sydney;
- on 15 June 2016, three deposits of $7,500 (totalling $22,500) in favour of Customer 36 at three different bank branches in Sydney;
- on 17 June 2016, 25 deposits of $8,000 (totalling $200,000) in favour of Customer 36 at 25 different bank branches in Sydney;
- on 20 June 2016, one deposit of $6,500 and 11 deposits of $8,500 (totalling $100,000) in favour of Customer 36 at 12 different bank branches in Sydney; and
- on 24 June 2016, 13 deposits of $8,500 (totalling $110,500) in favour of Customer 36 at 13 different bank branches in Sydney.

Transactions indicative of an ML/TF typology – smurfing

Transactions involving Customer 36 were identified as indicative of the ML/TF typology of smurfing by an independent auditor in 2021. The audit identified 83 suspicious transactions made between 9 June 2016 and 24 June 2016 totalling $656,000:

- on 9 June 2016, 13 transaction of $7,500 each (totalling $97,500) in favour of Customer 36 at 13 different bank branches in Sydney;

- on 10 June 2016, eight transactions of $7,500 each (totalling $60,000) in favour of Customer 36 at eight different bank branches;
- on 14 June 2016, 12 transactions of $7,500 each (totalling $90,000) in favour of Customer 36 at 12 different bank branches;
- on 15 June 2016, three transactions of $7,500 each (totalling $22,500) in favour of Customer 36 at three different bank branches;
- on 17 June 2016, 23 transactions of $8,000 each (totalling $184,000) in favour of Customer 36 at 23 bank branches;
- on 20 June 2016, one transaction of $6,500 and 11 transactions of $8,500 each (totalling $100,000) in favour of Customer 36 at 12 bank branches; and
- on 24 June 2016, 12 transactions of $8,500 each (totalling $102,000) in favour of Customer 36 at 12 bank branches.

Transactions indicative of an ML/TF typology – cuckoo smurfing

Transactions involving Customer 36 were identified as indicative of the ML/TF typology of cuckoo smurfing by an independent auditor in 2020 and 2021.

On 29 June 2016, Customer 36 received a telegraphic transfer of $475,485 at Crown Melbourne through a Southbank account from a third party. This transaction was indicative of the ML/TF typology of cuckoo smurfing.

The audit identified 14 transactions that occurred on 30 June 2016, totalling $585,000 comprising cash deposits and transfers to the Southbank accounts from a foreign money remitter. These transactions were indicative of the ML/TF typology of cuckoo smurfing.

Transactions indicative of an ML/TF typology – parked funds

From 12 May 2020 to at least 18 June 2021, Customer 36's safekeeping account had a dormant balance of $56,428. This was indicative of the ML/TF typology of parked funds.

Transactions indicative of an ML/TF typology – junket operator

In 2021, an independent auditor identified Customer 36 as responsive to an ML/TF "risk area" as a result of Customer 36's activity as a junket operator. The independent auditor noted that junkets are high risk for casino ML/TF activity and therefore customers identified as junket operators, including Customer 36, presented a higher ML/TF risk to Crown Melbourne and Crown Perth.

Ongoing customer due diligence

1560. On and from June 2016, on multiple occasions, the provision of designated services to Customer 36 raised red flags reflective of higher ML/TF risks as a result of Customer 36's significant junket activities, which involved high turnover.

Particulars

See paragraph 477

Customer 36's junket activities in 2016

Customer 36 operated several junkets including:

- in June 2016 with a loss of $1,320,390: SMR dated 6 June 2016; and
- in August 2016 with a turnover of $28,523,400. Customer 36 was a key player in the junket and had a personal turnover of $971,700 with a loss of $108,700.

On 4 August 2016, Customer 36 transferred $1,058,450 to a key player in his Crown Melbourne junket at settlement.

Customer 36's junket activities in 2017

By July 2017, Customer 36's junket turnover at Crown Melbourne totalled $149,000,000 with a loss of $100,000. Customer 36's junket turnover at Crown Melbourne totalled $34,000,000 with a loss of $300,000.

Customer 36's junket activities in 2018

By March 2018, Customer 36's cumulative junket turnover at Crown Melbourne totalled $368,000,000 with a loss of $5,300,000. Customer 36 operated several junkets including:

- in March 2018 with a loss of $1,320,390: SMR dated 22 March 2018;
- between 3 November 2018 and 6 November 2018 with a turnover of $2,170,000 and win of $38,930; and
- between 2 November 2018 and 7 November 2018 with a turnover of HKD81,000 and win of HKD7,750.

In FY2018, Crown Melbourne recorded Customer 36's individual gaming activity and gaming activity on junket programs run by Customer 36 as cumulative turnover of $217,605,400 with a loss of $6,881,410.

On 17 March 2018, Customer 36 transferred AU$1,026,299 in a foreign currency into his DAB account as front money.

On 1 November 2018, Customer 36 was extended a credit line of $5,000,000 with a TTO of $8,000,000.

On 3 November 2018 and 4 November 2018, a key player in Customer 36's Crown Perth junket played three losing shoes of

baccarat totalling HKD36,670,000 with average bets of over HKD1,000,000.

Customer 36's junket activities in 2019

In FY2019, Crown Melbourne recorded Customer 36's individual gaming activity and gaming activity on junket programs run by Customer 36 as cumulative turnover of $295,905,506 with a win of $1,902,999.

In FY2019, Crown Perth recorded Customer 36's individual gaming activity and gaming activity on junket programs run by Customer 36 as cumulative turnover of $66,503,637 with a win of $3,644,672. Customer 36 operated several junkets including:

- between 25 October 2019 and 2 November 2019, Customer 36 operated a junket with turnover of $54,030,000 and a win of $175,630; and
- between 25 October 2019 and 2 November 2019, Customer 36 operated a second junket with turnover of HKD84,000 and a loss of HKD19,200.

On 6 March 2019, Customer 36 was again approved for a credit line of $5,000,000 with a TTO of $8,000,000.

Customer 36's junket activities in 2020

In FY2020, Crown Perth recorded Customer 36's individual gaming activity and gaming activity on junket programs run by Customer 36 as cumulative turnover of $4,888,600 with a win of $381,465.

By September 2020, Customer 36's junket had a turnover at Crown Melbourne of $663,000,000 with a loss of $800,000.

By September 2020, Customer 36's junket had a turnover at Crown Perth of $100,000,000 with a loss of $3,800,000.

1561. On and from June 2016, on multiple occasions, designated services provided to Customer 36 raised red flags reflective of higher ML/TF risks as a result of transactions involving Customer 36 that were indicative of ML/TF typologies and vulnerabilities.

Particulars

See paragraph 24.

Between 9 June 2016 and 24 June 2016, $710,500 was deposited in favour of Customer 36's junket in a series of sub-threshold transactions made at numerous banks and branches indicative of the ML/TF typology of structuring. Many of those transactions, totalling $656,000, were indicative of the ML/TF typology of smurfing: see particulars to paragraph 1559.

Between 24 June 2016 and 28 June 2016, Crown Melbourne received 14 third party transactions totalling $586,000 from a foreign money changer. Crown Melbourne understood that the funds likely were deposited by Customer 36 to the money

changer which then made one deposit of $475,000 and 13 deposits of $8,500 at numerous bank branches in Sydney. Crown Melbourne received a telegraphic transfer acknowledgement form in respect of this sum: SMR dated 7 July 2016. These transactions were indicative of the ML/TF typologies of cuckoo smurfing and structuring.

1562. On and from June 2016, on multiple occasions, designated services provided to Customer 36 raised red flags reflective of higher ML/TF risks as a result of complex, unusually large transactions involving Customer 36 and unusual patterns of transactions by Customer 36 which had no apparent economic or visible lawful purpose including numerous third party transactions.

Particulars

See paragraph 450, 451 and 456ff.

Unusual transactions and patterns of transactions in 2016

In 2016, Crown Melbourne recorded Customer 36's individual rated gaming activity as a buy-in of $10,357,400 with a loss of $364,920.

Between 2 August 2016 and 3 August 2016, Customer 36 made a chip cash in of $20,650 and an account deposit of $24,000 at Crown Melbourne.

On 18 September 2016, Customer 36 transferred $50,000 to a Crown Melbourne patron.

Large and unusual third party transactions in 2016

Between 9 June 2016 and 20 June 2016, $656,000 was deposited in favour of Customer 36's junket in a series of sub-threshold transactions made at numerous banks and branches indicative of the ML/TF typology of smurfing: see particulars to paragraph 1559.

Crown Melbourne received copies of the deposit receipts on 24 June 2016: SMR dated 24 June 2016. As at 27 June 2016, Crown Melbourne were unsure who the beneficiary of the deposit was. It was thought that the beneficiary was either Customer 36 or Customer 34. The instructions for the deposits came from a foreign money changer: SMR dated 28 June 2016. The funds were used to repay at debt owed by Customer 36 at Crown Melbourne.

On 3 August 2016, Customer 36's Crown Melbourne junket sent a telegraphic transfer of $60,000 to a third party who was not a key player under any recent Customer 36 junket: SMR dated 4 August 2016.

Unusual transactions and patterns of transactions in 2017

In 2017, Crown Melbourne recorded Customer 36's individual rated gaming activity as a buy-in of $945,000 with a win of $83,165.

Unusual transactions and patterns of transactions in 2018

In 2018, Crown Melbourne recorded Customer 36's individual rated gaming activity as a buy-in of $8,101,295 with a loss of $7,312,640.

On 21 March 2018, Customer 36 made a chip account deposit of $25,000 at Crown Melbourne.

On 8 August 2018, Customer 36 transferred $18,527 from his Crown Perth DAB account to Crown Melbourne for his credit.

Large and unusual third party transactions in 2018

On 9 November 2018, Customer 36 sent a telegraphic transfer of a large sum in a foreign currency to the account of a foreign company, Company 12, associated with a casino cruise line. The casino cruise line was associated with the same corporate group that owned and operated a foreign casino at which Crown Perth understood that Customer 36 was a junket operator. The transaction narrative identified that the transfer was for the credit of Customer 36.

Unusual transactions and patterns of transactions in 2019

In 2019, Crown Melbourne recorded Customer 36's individual rated gaming activity as a buy-in of $45,249,089 with a win of $2,302,614.

On 25 October 2019, Customer 36 left two personal cheques of $1,000,000 and a large sum in a foreign currency at the Crown Perth Cage.

On 27 November 2019, Customer 36 sent a telegraphic transfer of $220,000 from his Crown Perth DAB account to Crown Melbourne for Person 20, a junket operator who used the funds to repay a debt at Crown Melbourne. Crown Perth understood that Customer 36 and Person 20 were business partners and junket operators together at a foreign casino. However, no other reason for the transfer was known: SMR dated 27 November 2019.

Large and unusual third party transactions in 2019

On 5 April 2019, Customer 36 sent a telegraphic transfer of a large sum in a foreign currency to the account of a foreign company, Company 12, associated with a casino cruise line. The casino cruise line was associated with the same corporate group that owned and operated a foreign casino at which Crown Perth understood that Customer 36 was a junket operator.

1563. At no time did Crown Melbourne or Crown Perth undertake appropriate risk-based customer due diligence with respect to Customer 36 with a view to identifying, mitigating and managing the ML/TF risks posed by the provision of designated services on and from June 2016.

a. At no time did Crown Melbourne and Crown Perth take appropriate steps to determine whether Customer 36's source of wealth/funds was legitimate.

b. At no time did Crown Melbourne or Crown Perth take appropriate steps to identify or analyse the ML/TF risks of Customer 36's transactions or to consider whether they had a lawful purpose.

c. With the exception of two transactions in June 2016 and April 2019, Crown Melbourne and Crown Perth gave no consideration at any time to whether large and high risk transactions should be processed. In June 2016 and April 2019, Crown Melbourne considered suspicious transactions involving Customer 36 but took no steps to prevent the transactions being processed or to ensure that the transactions had a lawful purpose.

d. On each occasion prior to June 2021 that senior management considered whether to continue the business relationship with Customer 36, senior management failed to give adequate consideration to whether the ML/TF risks posed by Customer 36 were within Crown Melbourne's risk appetite.

e. Prior to the decision to issue Customer 36 with an NRL in June 2021, there is no record of senior management considering whether continuing the business relationship with Customer 36 was within Crown Perth's ML/TF risk appetite in light of the ML/TF risks posed by Customer 36.

Particulars

Section 36(1)(a) of the Act.

The due diligence steps taken with respect to Customer 36 included:

Wealth and risk intelligence reports

In August 2016, December 2016, March 2018, April 2019 and May 2019, Crown Melbourne obtained wealth reports in respect of Customer 36. The reports identified Customer 36's business interests, including that he was an experienced overseas junket operator with a licence to operate junkets in multiple jurisdictions.

In May 2017 and December 2019, Crown obtained risk intelligence reports in respect of Customer 36.

In September 2019, Crown Melbourne and Crown Perth obtained a wealth report in respect of Customer 36.

At no point, as a result of these reports, did Crown Melbourne or Crown Perth appropriately consider the ML/TF risks of the source of Customer 36's wealth/funds or whether an ongoing business relationship with Customer 36 was within their ML/TF risk appetite.

Other due diligence searches – Crown Melbourne

Between May 2017 and October 2020, Crown Melbourne conducted risk intelligence searches, company searches and open searches in respect of Customer 36.

At no point, as a result of these searches, did Crown Melbourne appropriately consider the ML/TF risks of the source of Customer 36's wealth/funds or whether an ongoing business relationship with Customer 36 was within its ML/TF risk appetite.

Other due diligence searches – Crown Perth

Between November 2018 and November 2019, Crown Perth conducted risk intelligence and company searches in respect of Customer 36.

By November 2019, Crown Perth was aware that Customer 36 was the sole junket operator at a foreign casino: SMR dated 27 November 2019.

At no point, as a result of these searches, did Crown Perth appropriately consider the ML/TF risks of the source of Customer 36's wealth/funds or whether an ongoing business relationship with Customer 36 was within its ML/TF risk appetite.

Considerations of large and suspicious transactions

Following the series of cash deposits leading up to 24 June 2016 to Customer 36's junket account totalling $656,000 (see paragraph 1559), a Crown Melbourne Credit control coordinator (VIP International) requested that the money changer provide a letter or receipt confirming the deposit for reporting purposes. However, Customer 36's personal assistant was only able to provide the money changer's business card. Nonetheless, the transaction was processed.

Following the telegraphic transfer of a large sum in a foreign currency on 5 April 2019 to Company 12, Crown Melbourne conducted a search of that company which returned an address in a foreign country. There is no indication that Crown Melbourne conducted appropriate searches to identify the foreign company. The foreign company is associated with the same corporate group that owned and operated a foreign casino at which Crown Perth understood that Customer 36 was a junket operator.

At no point, as a result of these searches, did Crown Melbourne appropriately consider the ML/TF risks of the source of Customer 36's wealth/funds or whether an ongoing business relationship with Customer 36 was within its ML/TF risk appetite.

Senior management engagement

On July 2017, March 2018, October 2019, Crown prepared a junket profile in respect of Customer 36's junket. Each profile recommended Crown continue to conduct business with Customer 36.

The junket profiles did not appropriately consider the ML/TF risks of the source of Customer 36's wealth/funds.

None of these steps were proportionate to the ML/TF risks reasonably posed by Customer 36 on and from 1 March 2016.

The April – June 2021 review

Between April 2021 and June 2021, Crown conducted a range of due diligence and open source searches in respect of Customer 36 and key players on his junkets.

On 22 June 2021, as a result of the SPR process, Crown Melbourne issued a WOL in respect of Customer 36: see particulars to paragraph 1234.

On 22 June 2021, as a result of the SPR process, Crown Perth issued an NRL in respect of Customer 36: see particulars to paragraph 1234.

Enhanced customer due diligence

1564. Having formed a suspicion for the purposes of s41 of the Act, Crown Melbourne gave the AUSTRAC CEO SMRs with respect to Customer 36 on:

a. 6 June 2016;

b. 24 June 2016;

c. 28 June 2016;

d. 7 July 2016;

e. 4 August 2016;

f. 22 March 2018; and

g. 5 April 2019.

Particulars

These SMRs described telegraphic transfers to third parties and company accounts, high individual and annual losses for key players in Customer 36's junket, funds being repeatedly deposited below the reporting threshold through a money changer and the amount of cash key players in Customer 36's junket were prepared to carry.

1565. Having formed a suspicion for the purposes of s41 of the Act, Crown Perth gave the AUSTRAC CEO SMRs with respect to Customer 36 on:

a. 27 November 2019; and

b. 22 October 2020.

Particulars

The SMRs described telegraphic transfers between junket operators and identified for the first time the transactions indicative of the ML/TF typology of structuring in November 2013: see particulars to paragraph 1553.

1566. On each occasion that Crown Melbourne or Crown Perth formed a suspicion with respect to Customer 36 for the purposes of s41 of the Act, it was required to apply its ECDD program to Customer 36.

Particulars

Rule 15.9(3) of the Rules.

1567. Crown Melbourne and Crown Perth did not carry out appropriate risk-based ECDD measures with respect to Customer 36 on each occasion that Crown Melbourne or Crown Perth formed a suspicion with respect to Customer 36 for the purposes of s41 of the Act.

a. There are no records of ECDD being conducted by Crown Melbourne after it gave the AUSTRAC CEO any SMR.

b. There are no records of ECDD being conducted by Crown Perth after it gave the AUSTRAC CEO the SMR dated 27 November 2019: see paragraphs 664 and 685.

c. Crown Melbourne and Crown Perth did not take appropriate steps to obtain or analyse information about Customer 36's source of wealth/funds or to determine whether Customer 36's source of wealth/funds was legitimate: see paragraph 667.

d. Appropriate risk-based steps were not taken to analyse and monitor Customer 36's transactions – both past and future – including to understand their economic purpose: see paragraphs 590 and 666.

e. On each occasion prior to June 2021 that senior management considered whether to continue the business relationship with Customer 36, senior management failed to give adequate consideration to whether the ML/TF risks posed by Customer 36 were within Crown Melbourne's risk appetite.

f. Prior to the decision to issue Customer 36 with an NRL in June 2021, there is no record of senior management considering whether continuing the business relationship with Customer 36 was within Crown Perth's ML/TF risk appetite in light of the ML/TF risks posed by Customer 36: see paragraph 668ff.

Particulars

Rules 15.9(3), 15.10(1)(c), (d), (2), (5) and (6) of the Rules.

In respect of the 24 and 28 June 2016 SMRs and the 5 April 2019 SMR, Crown Melbourne considered the suspicious transactions involving Customer 36 but took no steps to conduct appropriate due diligence in respect of any of them.

See particulars to paragraph 1563.

1568. By reason of the matters pleaded from paragraphs 1547 to 1567, on and from June 2016, Crown Melbourne and Crown Perth:

a. did not monitor Customer 36 in relation to the provision of designated services, with a view to identifying, mitigating and managing the ML/TF risks reasonably faced; and

b. did not do so in accordance with rr 15.5 and 15.9 of the Rules.

1569. By reason of the matters pleaded at paragraph 1568, Crown Melbourne and Crown Perth contravened s36(1) of the Act on and from June 2016 to June 2021 with respect to Customer 36.

Particulars

Section 36(1) of the Act is a civil penalty provision: s36(2) of the Act.

Customer 37

1570. Customer 37 has been a customer of Crown Melbourne since February 2006.

1571. From at least December 2006, Crown Melbourne provided Customer 37 with designated services within the meaning of table 1 and table 3, s6 of the Act.

Particulars

On 1 February 2006, Crown Melbourne opened a DAB account and a safekeeping account for Customer 37.

On 5 April 2019, Crown Melbourne opened a credit facility for Customer 37, which was closed on 20 June 2021.

In 2006, Crown Melbourne recorded Customer 37's individual rated gaming activity to be buy-in of $100,000, average bet of $10,827 and loss of $225,850. Customer 37 had no rated gaming activity between 2007 and 2018.

In 2019, Crown Melbourne recorded Customer 37's individual rated gaming activity to be buy-in of $5,936,300, average bet of $122,822 and loss of $6,085,750.

The ML/TF risks posed by Customer 37

1572. By 1 March 2016, higher ML/TF risks were indicated by the nature and purpose of Customer 37's business relationship with Crown Melbourne and the nature of the transactions he had been conducting.

Particulars

Section 36(1)(a), (b) of the Act and Chapter 15 of the Rules.

In 2008, Customer 37 was a junket player. He received designated services through the channel of junket programs. This channel lacked transparency: see paragraph 477.

In 2006, Crown Melbourne recorded Customer 37's individual rated gaming activity to be buy-in of $100,000, average bet of $10,827 and loss of $225,850.

In 2008, Customer 37 participated in one junket program and recorded a turnover of $42,860,700 with a loss of $3,392,075.

By 1 March 2016, no due diligence steps had been taken in respect of Customer 37.

1573. By mid-2019, Customer 37 should have been recognised by Crown Melbourne as a high risk customer by reason of the matters pleaded at paragraphs 1572, 1576, 1577, 1578 and 1580.

Particulars

Section 36(1)(a), (b) of the Act and Chapter 15 of the Rules.

1574. At no time was Customer 37 rated high risk by Crown Melbourne.

Particulars

On various occasions between 23 April 2019 and 21 May 2019, Crown Melbourne assessed Customer 37 as moderate risk.

In 2019, Customer 37 engaged in significant individual gaming activity at Crown Melbourne, was granted a $3,000,000 credit facility and received telegraphic transfers from international third parties totalling over $5,000,000.

See paragraph 120.

1575. At all times on and from mid-2019, Customer 37 should have been recognised by Crown Melbourne as a high risk customer by reason of the matters pleaded at paragraphs 1572, 1576, 1577, 1578 and 1580.

Particulars

Section 36(1)(a), (b) of the Act and Chapter 15 of the Rules.

1576. On and from 2019, designated services provided to Customer 37 posed higher ML/TF risks including because the provision of designated services to Customer 37 involved a combination of the following factors:

a. Customer 37 received high value financial (table 1, s6) and gaming services (table 3, s6);

b. in 2019, Customer 37 had a buy-in of $5,936,300, average bet of $122,822 and loss of $6,085,750;

c. designated services provided to Customer 37 involved large transfers to and from third parties, including foreign money changers and unknown third parties: see paragraph 456ff;

d. designated services provided to Customer 37 involved large cross-border movements of funds, including through the Southbank accounts: see paragraph 239;

e. large values were transferred to and from Customer 37's bank accounts and his DAB account, and to other customers' DAB accounts, involving the provision by Crown Melbourne of designated services within the meaning of items 31 and 32, table 1, s6 of the Act: see paragraph 411ff;

f. at various times, Customer 37 was provided with significant amounts of credit upon request, up to limits of $3,000,000: see paragraph 280ff;

g. in 2019, when initially precluded from opening a credit facility at Crown Melbourne, Customer 37 requested to open a credit facility in the name of his personal assistant accessible to both patrons and Crown Melbourne took steps to facilitate that request;

h. in 2021, Customer 37 refused to complete a source of wealth declaration;

i. Customer 37 engaged in transactions indicative of ML/TF typologies and vulnerabilities, including the use of third party agents and cuckoo smurfing: see paragraph 24;

j. these transactions took place against the background of Customer 37's participation in a junket program in 2008 where he recorded a turnover of $42,860,700 with a loss of $3,392,075;

k. by September 2021, Crown Melbourne was aware of media reports that named Customer 37 as a person involved in land purchases without the necessary approvals in a foreign country; and

l. by reason of the matters set out at subparagraphs a. to k. above, there were higher ML/TF risks associated with Customer 37's source of wealth/funds.

Monitoring of Customer 37's transactions

1577. At no time did Crown Melbourne appropriately monitor Customer 37's transactions on a risk-basis.

Particulars

Section 36(1)(a), (b) of the Act and Rules 15.4 to 15.8 of the Rules.

Crown Melbourne did not apply appropriate risk-based transaction monitoring to designated services provided to Customer 37: see paragraphs 590ff and 629 to 642.

Customer 37's transactions involved repeated transactions indicative of ML/TF typologies and vulnerabilities that were not detected prior to a 2021 lookback. Had appropriate risk-based transaction monitoring been applied, these transactions could have been identified earlier: see paragraphs 686 and 687.

The following transactions involving Customer 37 were identified as indicative of the ML/TF typology of use of third party agents by an independent auditor in 2020 and 2021:

- on 20 April 2019, a $2,350,000 transfer to Customer 37 through a Southbank account. This transfer came from an overseas third party who Crown Melbourne understood to be Customer 37's personal assistant;
- on 20 May 2019, a $2,975,330 transfer to Customer 37 through a Southbank account. This transfer came from a third party in a foreign country, who was understood to be an employee of a foreign company affiliated with Customer 37. The purpose of the transaction was to settle Customer 37's outstanding CCF balance. The transaction was made through a foreign money changer. This transaction was also indicative of the ML/TF typology of cuckoo smurfing; and
- on 24 January 2020, a $364,784 transaction from Customer 37 to another Crown patron through a Crown Melbourne bank account.

In 2021, an independent auditor identified Customer 37 as having the same patron identifiers as another Crown Melbourne customer, which the auditor considered to be indicative of an ML/TF typology.

Ongoing customer due diligence

1578. On and from 2019, on multiple occasions, the provision of designated services to Customer 37 by Crown Melbourne raised red flags reflective of higher ML/TF risks.

Particulars

Gaming activity

In 2019, Crown Melbourne recorded Customer 37's individual rated gaming activity as escalating to a cumulative buy-in of $5,936,300, average bet of $122,822 and loss of $6,085,750.

Large and unusual transactions

On 18 April 2019, Customer 37 transferred $150,000 to his DAB account. On the same day, Customer 37 transferred $75,000 each to two other Crown Melbourne patrons.

On 22 April 2019, Customer 37 made a deposit of $77,500 into his DAB account.

Other red flags

In January and February 2019, following a request from Customer 37, the Senior Vice President (International Business Operations) arranged for a CCF for $3,000,000 in the name of Customer 37's personal assistant that could be accessed by both Customer 37 and his personal assistant. This was due to the fact that Customer 37's business interests were exclusively in a foreign country and Crown Melbourne's policies precluded Customer 37 from being granted a CCF.

On 5 April 2019, Crown Melbourne opened a credit facility in Customer 37's name after Customer 37 provided additional evidence of business interests in another foreign country. The CCF was approved by the Chief Legal Officer (Australian Resorts), the Chief Executive Officer (Australian Resorts) and a Crown Resorts Ltd director.

In May 2021, Customer 37 refused to complete a source of wealth declaration.

1579. At no time did Crown Melbourne undertake appropriate risk-based customer due diligence with respect to Customer 37 with a view to identifying, mitigating and managing the ML/TF risks posed by the provision of designated services on and from 2019.

a. At no time did Crown Melbourne take appropriate steps to understand whether Customer 37's source of wealth/funds was legitimate.

b. At no time did Crown Melbourne take appropriate steps to identify or analyse the ML/TF risks of Customer 37's transactions or to consider whether they had a lawful purpose.

c. Crown Melbourne gave no consideration at any time to whether large and high risk transactions involving Customer 37 should be processed.

d. At no time did senior management consider whether continuing the business relationship with Customer 37 was within Crown Melbourne's ML/TF risk appetite.

Particulars

Section 36(1)(a) of the Act.

The due diligence steps taken with respect to Customer 37 included:

2019 credit application

For the purpose of approving Customer 37's application for a credit facility of $3,000,000 in 2019, Crown Melbourne conducted a number of checks for the purpose of assessing Customer 37's creditworthiness.

The information compiled as a result of these credit checks was provided to the Senior Vice President (International Business), the Chief Legal Officer (Australian Resorts), the Chief Executive Officer (Australian Resorts) and a Crown Resorts Ltd director with a recommendation that Customer 37 be allowed to apply for credit. The credit application was approved.

These steps taken were not directed at considering or addressing the ML/TF risk reasonably posed by Customer 37. Crown Melbourne did not appropriately consider the ML/TF risks of the source of Customer 37's wealth/funds or whether an ongoing business relationship with Customer 37 was within its ML/TF risk appetite.

August 2020 review

In August 2020, Crown Melbourne conducted Australian company searches, risk intelligence searches and open source media searches in respect of Customer 37.

September 2020 KYC profile

In September 2020, Crown Melbourne prepared a KYC profile in respect of Customer 37. The profile identified that Customer 37's level of play was extremely high and suggested that Customer 37 be flagged for regular AML review. There is no indication that such reviews occurred.

The KYC profile suggested that a wealth report be obtained in respect of Customer 37 in order to confirm that his source of wealth was consistent with his buy in. There is no record of a wealt report being obtained.

July 2021 media articles

From at least 3 September 2021, Crown Melbourne was aware of two news articles dated 22 July 2021 which related to Customer 37. The articles reported that a foreign court found that a company did not seek approval prior to a sensitive land purchase made on behalf of Customer 37, who was an overseas investor.

August 2021 Significant Player Review

On 12 August 2021, Crown Melbourne applied the SPR process (see particulars to paragraph 1234) to Customer 37 and recorded that Crown Melbourne was unable to verify Customer 37's KYC information, or that there were discrepancies with Customer 37's KYC information. The form used for the SPR process has no input for (and therefore no record of) Customer 37's refusal to complete a SOF/SOW declaration. No further steps were taken.

None of these steps were proportionate to the ML/TF risks reasonably posed by Customer 37 on and from 2019.

Enhanced customer due diligence

1580. Having formed a suspicion for the purposes of s41 of the Act, Crown Melbourne gave the AUSTRAC CEO SMRs with respect to Customer 37 on:

a. 23 April 2019; and

b. 21 May 2019.

Particulars

Each SMR described Customer 37's annual losses, large third party transactions and the amount of cash that Customer 37 was prepared to carry.

1581. On each occasion that Crown Melbourne formed a suspicion with respect to Customer 37 for the purposes of s41 of the Act, it was required to apply its ECDD program to Customer 37.

Particulars

Rule 15.9(3) of the Rules.

1582. Crown Melbourne did not carry out appropriate risk-based ECDD measures with respect to Customer 37 on each occasion that Crown Melbourne formed a suspicion with respect to Customer 37 for the purposes of s41 of the Act.

a. There are no records of ECDD being conducted following the lodgement of SMRs on 23 April 2019 and 21 May 2019: see paragraphs 664 and 685.

b. Appropriate risk-based steps were not taken to obtain or analyse information about Customer 37's source of wealth/funds: see paragraph 667.

c. Appropriate risk-based steps were not taken to analyse and monitor Customer 37's transactions – both past and future – including to understand their economic purpose: see paragraphs 590 and 666.

d. At no time did senior management consider whether continuing the business relationship with Customer 37 was within Crown Melbourne's ML/TF risk appetite: see paragraph 668ff.

Particulars

Rules 15.9(3), 15.10(1)(c), (d), (2), (5) and (6) of the Rules.

See particulars to paragraph 1579.

1583. By reason of the matters pleaded from paragraphs 1570 to 1582, on and from 2019 Crown Melbourne:

a. did not monitor Customer 37 in relation to the provision of designated services, with a view to identifying, mitigating and managing the ML/TF risks reasonably faced; and

b. did not do so in accordance with rr 15.5 and 15.9 of the Rules.

1584. By reason of the matters pleaded at paragraph 1583, Crown Melbourne contravened s36(1) of the Act on and from 2019 with respect to Customer 37.

Particulars

Section 36(1) of the Act is a civil penalty provision: s36(2) of the Act.

Customer 38

1585. Customer 38 was a customer of Crown Melbourne from March 2012 to 29 August 2020.

1586. From at least April 2016 to 29 August 2020, Crown Melbourne provided Customer 38 with designated services within the meaning of table 1 and table 3, s6 of the Act.

Particulars

On 14 April 2016, Crown Melbourne opened a DAB account and safekeeping account (AUD) for Customer 38 under two PIDs.

Customer 38 was a premium program player.

In 2015, Crown Melbourne recorded Customer 38's individual gaming activity to be a loss of $61,875: SMR dated 24 June 2016.

Between 2016 and 2017, Crown Melbourne recorded Customer 38's individual gaming activity to be a loss of $2,177,130.

On 29 August 2020, Crown Melbourne issued an indefinite WOL in respect of Customer 38.

1587. Customer 38 was a customer of Crown Perth from 17 November 2016 to 31 August 2021.

1588. From at least 17 November 2016 to August 2021, Crown Perth provided Customer 38 with designated services within the meaning of table 1 and table 3, s6 of the Act.

Particulars

On 17 November 2016, Crown Perth opened a DAB account and a safekeeping account (AUD) for Customer 38 under his PID.

On 18 November 2016, Crown Perth opened a second DAB account and safekeeping account (AUD) for Customer 38 under a second PID.

On 18 November 2016, Crown Perth assigned Customer 38 to its premium program player.

On 11 March 2017, Crown Perth opened a FAF (AUD) for Customer 38 under two PIDs. The facility was closed by Crown Perth on 14 March 2017.

On 31 August 2021, Crown Perth issued an NRL in respect of Customer 38.

The ML/TF risks posed by Customer 38

1589. By November 2018, Customer 38 should have been recognised by Crown Melbourne and Crown Perth as a high risk customer for the reasons pleaded at paragraphs 1593, 1594, 1595, 1596, 1597, 1598 and 1600.

1590. At no time was Customer 38 rated as high risk by Crown Melbourne.

Particulars

On various occasions between 19 April 2016 and 14 December 2018, Crown Melbourne assessed Customer 38 as moderate risk.

See paragraph 120.

1591. At no time was Customer 38 rated as high risk by Crown Perth.

Particulars

On various occasions between 12 May 2017 and 5 December 2018, Crown Perth assessed Customer 38 as moderate risk.

See paragraph 120.

1592. At all times on and from November 2018, Customer 38 should have been recognised by Crown Melbourne and Crown Perth as a high risk customer by reason of the matters pleaded at paragraphs 1593, 1594, 1595, 1596, 1597, 1598 and 1600.

Particulars

Section 36(1)(a), (b) of the Act and Chapter 15 of the Rules.

1593. By late 2016 designated services provided to Customer 38 posed higher ML/TF risks including because the provision of designated services to Customer 38 involved a combination of the following factors:

a. Customer 38 received high value financial (table 1, s6) and gaming services (table 3, s6);

b. by 2017, Crown Melbourne recorded Customer 38's individual rated gaming activity to be a loss of $2,239,005;

c. Customer 38's average bet increased from $17,448 in 2016 to $48,816 in 2017;

d. designated services provided to Customer 38 involved large transfers to and from third parties, including foreign remittance service providers and unknown third parties: see paragraph 456ff;

e. designated services provided to Customer 38 involved large cross-border movements of funds, including through the Southbank accounts: see paragraph 239;

f. between 18 April 2016 and 9 July 2018, Customer 38 received telegraphic transfers totalling AU$13,570,047 in a foreign currency and sent telegraphic transfers totalling AU$18,767,889 in a foreign currency via the Southbank accounts;

g. large values of funds were transferred to and from Customer 38's bank accounts and his DAB account, and to and from other customers' DAB accounts, involving designated

services within the meaning of items 31 and 32, table 1, s6 of the Act: see paragraph 411ff;

h. Customer 38 engaged in transactions indicative of ML/TF typologies and vulnerabilities, including quick turnover of money (without betting), cuckoo smurfing, transfers to third parties (including companies) and use of overseas remittance services: see paragraph 24;

i. by no later than May 2017, Crown Perth was suspicious that Customer 38 was using a third party, Person 51, as a money changer;

j. by 2 November 2018, a foreign bank had expressed money laundering concerns to Crown Melbourne in respect of the large volume and value of Customer 38's telegraphic transfers and was questioning the source of funds; and

k. by reason of the matters set out at subparagraphs a. to j. above, there were higher ML/TF risks associated with Customer 38's source of wealth/funds.

Monitoring of Customer 38's transactions

1594. At no time did Crown Melbourne or Crown Perth appropriately monitor Customer 38's transactions on a risk-basis.

Particulars

Section 36(1)(a), (b) of the Act and Rules 15.4 to 15.8 of the Rules.

Crown Melbourne and Crown Perth did not apply appropriate risk-based transaction monitoring to designated services provided to Customer 38: see paragraphs 590ff and 629 to 642.

Customer 38's transactions involved repeated transactions indicative of ML/TF typologies and vulnerabilities that were not detected prior to two separate independent audits in 2020 and 2021. Had appropriate risk-based transaction monitoring been applied, these transactions could have been identified earlier: see paragraphs 686 and 687.

Transactions indicative of ML/TF typologies – quick turnover (without betting)

Transactions involving Customer 38 were identified as indicative of the ML/TF typology of quick turnover of funds (without betting) by an independent auditor in 2021. The following transactions of Customer 38's were identified as involving the deposit of cash or telegraphic transfers and withdrawal of 70% or more of the deposit amount within a 48 hour period:

- on 4 July 2016, Customer 38 deposited $200,000 by telegraphic transfer, then withdrew $254,130 from his DAB account by telegraphic transfer on the same day;
- on 25 November 2016, Customer 38 deposited $500,000 by telegraphic transfer, then withdrew $500,000 from his DAB account by telegraphic transfer on the same day;

- between 3 and 5 January 2017, Customer 38 deposited $20,000 in cash, then withdrew $200,000, $500,000 and $1,518,097 from his DAB account in separate telegraphic transfer transactions;
- on 2 March 2017, Customer 38 deposited $552,741 by telegraphic transfer, then withdrew $552,741 from his DAB account on the same day;
- on 20 April 2017, Customer 38 deposited $102,232 and $337,692 in two separate telegraphic transfers, then withdrew $450,000 from his DAB account by telegraphic transfer on the same day;
- on 23 April 2017, Customer 38 deposited $1,154,706 by telegraphic transfer, then withdrew $1,096,096 from his DAB account by telegraphic transfer on the same day;
- on 24 April 2017, Customer 38 deposited $548,046 by telegraphic transfer, then withdrew $548,046 from his DAB account by telegraphic transfer on the same day;
- on 27 April 2017, Customer 38 deposited $136,974, $136,974 and $136,974, then withdrew $480,000 from his DAB account by telegraphic transfer on the same day;
- on 1 May 2017, Customer 38 deposited $100,000 by telegraphic transfer, then withdrew $36,247 in in cash and $100,000 by telegraphic transfer from his DAB account on the same day;
- on 8 May 2017, Customer 38 deposited $1,157,985 by telegraphic transfer, then withdrew $545,208 and $545,208 by telegraphic transfer from his DAB account on the same day, then a further $20,000 the following day;
- on 26 August 2017, Customer 38 deposited $907,407 by telegraphic transfer, then withdrew $907,407 by telegraphic transfer from his DAB account on the same day;
- on 5 July 2017, Customer 38 deposited $90,547, $135,821, $135,821, and $150,000 by telegraphic transfer, then withdrew $500,000 by telegraphic transfer from his DAB account on the same day; and
- on 9 July 2017, Customer 38 deposited $220,660 by telegraphic transfer, then withdrew $105,283 and $135,821 by telegraphic transfer from his DAB account on the same day.

Transactions indicative of ML/TF typologies – use of third party agents

Transactions involving Customer 38 were identified as indicative of the ML/TF typology of the use of third party agents by an independent auditor in 2021:

- on 16 June 2017, Customer 38 deposited $499,993 into a Southbank account, using a transaction narrative that referred to a third party;

- on 21 June 2017, Customer 38 deposited $915,880 into a Southbank account, using a transaction narrative that referred to a third party; and
- on 28 August 2017, Customer 38 deposited $907,400 into a Southbank account, using a transaction narrative that referred to a third party.

Transactions indicative of ML/TF typologies – use of potential shell companies

Transactions involving Customer 38 were identified as indicative of the ML/TF typology of the use of a potential shell company, Company 11, by an independent auditor in 2021:

- on 20 October 2016, Customer 38 used a shell company to deposit $300,000 into a Southbank account;
- on 1 November 2016, Customer 38 used a shell company to deposit $300,000 into a Southbank account;
- on 2 November 2016, Customer 38 used a shell company to deposit $300,000 into a Southbank account;
- on 19 April 2017, Customer 38 used a shell company to deposit $337,691 into a Southbank account; and
- on 20 April 2017, Customer 38 used a shell company to deposit $102,231 into a Southbank account.

Ongoing customer due diligence

1595. By late 2016, on multiple occasions, the provision of designated services to Customer 38 by Crown Melbourne raised red flags reflective of higher ML/TF risks as a result of Customer 38's escalating levels of play and high turnover.

Particulars

By 24 October 2016, Customer 38 had visited Crown Melbourne 39 times. His total buy-in was $9,122,500 and his losses were $1,097,165. His average bet was $18,490: SMR dated 24 October 2016. His total buy-in as at 31 October 2016 had increased to $10,377,500. His losses had increased to $1,616,680: SMR dated 31 October 2016.

By late December 2016, Customer 38 had visited Crown Melbourne 64 times, with a total buy-in of $14,620,000 and losses of $3,172,870: SMR dated 23 December 2016.

Customer 38's average bet increased from $17,448 in 2016 to $48,816 in 2017: SMR dated 23 June 2017.

As at 10 March 2017, Crown Perth recorded Customer 38's individual rated gaming activity in FY2017 to be a turnover of $53,017,300 with wins of $1,730,130.

By 23 June 2017, Crown Melbourne recorded Customer 38's individual rated gaming activity to be a loss of $1,594,610: SMR dated 23 June 2017.

By 30 December 2017, Crown Melbourne recorded Customer 38's individual gaming activity to be a loss of $268,410: SMR dated 9 January 2018.

1596. By late 2016, on multiple occasions, the provision of designated services to Customer 38 by Crown Melbourne raised red flags reflective of higher ML/TF risks as a result of complex, unusually large transactions and unusual patterns of transactions which had no apparent economic or visible lawful purpose.

Particulars

See paragraphs 420ff and 456ff.

Large and unusual transactions and patterns of transactions in 2016

On 16 April 2016, Customer 38 deposited $18,005 in his DAB account and then withdrew $30,030 the following day.

On 5 September 2016, Crown Melbourne recorded a $400,000 transaction on Customer 38's DAB account with the transaction description "hotel payout".

On 6 September 2016, Customer 38 made three telegraphic transfers in a foreign currency to Crown Melbourne totalling AU$322,082.

On 14 September 2016, Customer 38 transferred AU$322,082 in a foreign currency from his DAB account to his personal account.

On 17 October 2016, Crown Melbourne recorded a $200,000 transaction on Customer 38's DAB account with the description "bank transaction" and a further $70,000 with the description "70K bank transaction approved".

Between 22 October 2016 and 23 October 2016, Customer 38 sent two telegraphic transfers in foreign currency in the amount of AUD$139,341 and AU$139,743 to his DAB account. In the same period, Customer 38 cashed out $247,720 in chips in 10 separate transactions.

Between 23 October 2016 and 24 October 2016, Crown Melbourne recorded a $200,000 transaction on Customer 38's DAB account. He also cashed out $22,450 in chips in two transactions.

On 28 October 2016, Customer 38 sent a telegraphic transfer in foreign currency in the amount of AU$139,341 to his DAB account.

On 29 October 2016, Customer 38 cashed out $41,300 of chips in two separate transactions.

On 31 October 2016 and 1 November 2016, Customer 38 made a cash deposit of $20,000 and $30,000 respectively into his DAB account.

On 19 December 2016, Customer 38 cashed out $14,600 of chips.

On 20 December 2016, Customer 38 withdrew $55,700 in cash from his DAB account.

On 22 December 2016, Customer 38 transferred AU$755,630 in foreign currency in six transactions to his DAB account.

On 23 December 2016, Customer 38 sent four telegraphic transfers in foreign currency to his DAB account totalling AUD$755,630.

Large and unusual transactions and patterns of transactions in 2017

On 4 January 2017, a Crown employee noted a suspicious pattern of transactions related to transfers from Customer 38's bank account in a foreign country, observing that Customer 38 would transfer additional funds when winning under the junket program, and transfer the initial front money to a third party.

On 10 March 2017, Customer 38 played on a premium program at Crown Perth. His buy-in was $500,000 with wins of $542,000. A commission of $31,168 was payable by Crown Perth to Customer 38 following the program (0.7% of his turnover of $4,452,000 for the visit).

On 19 March 2017, Customer 38 transferred $85,000 to another patron's DAB account (Person 52): SMR dated 18 April 2017.

On 16 April 2017, Customer 38 withdrew $70,000 in cash from his DAB account in three separate withdrawals.

On 17 April 2017, Customer 38 received eight telegraphic transfers in a foreign currency of AU$137,012 from his DAB account, totalling AU$1,096,096.

On 17 April 2017, Customer 38 transferred $100,000 to another Crown Melbourne customer, Person 52: SMR dated 18 April 2017.

On 5 May 2017, Crown Melbourne was aware that Customer 38 and Person 51 were friends and formed a suspicion that Customer 38 was using the third party Person 51 as a money changer. Crown Melbourne believed that the third party was also a Crown Melbourne customer: SMR dated 5 May 2017.

On 19 June 2017, Customer 38 transferred AU$565,188 in a foreign currency to his DAB account in four equal transactions.

On 21 June 2017, Customer 38 deposited $10,000 in cash into his DAB account.

On 22 June 2017, Customer 38's received $290,000 into his DAB account from another Crown Melbourne patron, Person 52.

Large and unusual transactions and patterns of transactions in 2018

On 5 January 2018, Customer 38 cashed out $12,000 of chips.

On 6 January 2018, Customer 38 received $125,000 into his DAB account from another Crown Melbourne patron, Person 52.

On 6 January 2018, Customer 38 deposited $21,000 into his DAB account and cashed out $10,000 of chips.

On 7 January 2018, Customer 38 withdrew $16,000 in cash from his DAB account.

On 21 April 2018, Customer 38 transferred $80,000 from his DAB account to another Crown Melbourne patron.

On 23 April 2018, Customer 38 transferred $100,000 from his DAB account to another Crown Melbourne patron.

Large and unusual transactions and patterns of transactions in 2019

Between 25 April 2019 and 2 May 2019, Customer 38 played on a program at Crown Melbourne. On 25 April 2019, Customer 38 made four telegraphic transfers of $46,030 to Crown Melbourne, which was used as front money ($184,120) for his program. Customer 38 turned over $2,711,000 on the program with losses of $127,680.

1597. By late 2016, on multiple occasions, the provision of designated services to Customer 38 raised red flags reflective of higher ML/TF risks as a result of Customer 38's frequent, large transactions with a number of third parties.

Particulars

See paragraph 456ff.

In 2016, Crown Melbourne recorded:

- one telegraphic transfer of $720,000 from Customer 38 to a third party;
- one telegraphic transfer of $83,584 from Customer 38 to an overseas third party: SMR dated 15 September 2016; and
- five telegraphic transfers from Customer 38 totalling $1,243,560 to a second third party, Person 51;

In 2017 and 2018, Crown Melbourne recorded:

- five telegraphic transfers totalling $766,106 from Customer 38 to a third party;
- 18 telegraphic transfers from Customer 38 totalling $6,912,389 to a second third party, Person 51; and
- one telegraphic transfer from Customer 38 to another third party for $39,115: SMR dated 14 December 2018.

1598. In November 2018, the provision of designated services to Customer 38 raised red flags reflective of higher ML/TF risks as a result of Crown Melbourne being aware that a foreign bank had expressed concerns about Customer 38 in connection with money laundering.

Particulars

On 2 November 2018, a foreign bank contacted Crown Melbourne expressing money laundering concerns over Customer 38's regular payments to Crown Melbourne totalling $15 million over 2017 and

2018 and requesting information, including how the funds were generated.

1599. At no time did Crown Melbourne or Crown Perth undertake appropriate risk-based customer due diligence with respect to Customer 38 with a view to identifying, mitigating and managing the ML/TF risks posed by the provision of designated services on and from 1 March 2016.

a. Despite receiving a query from a foreign bank in November 2018 regarding Customer 38 and querying his source of funds, no steps were taken for verify Customer 38's source of funds.

b. Despite Customer 38 making repeated large value transactions to a third party company and third party individual, no steps were taken to assess Customer 38's relationship with either third party, nor were any steps taken to assess the ML risks arising from Customer 38's relationship with and transfers to those third parties.

c. At no time did Crown Melbourne or Crown Perth take appropriate steps to understand Customer 38's source of wealth/funds and whether his source of wealth/funds was legitimate.

d. At no time did Crown Melbourne or Crown Perth take appropriate steps to identify or analyse the ML/TF risks of Customer 38's transactions or to consider whether they had a lawful purpose.

e. At no time did Crown Melbourne or Crown Perth take steps to understand the relationship between Customer 38 and the third parties to whom he regularly transferred funds.

f. At no time did Crown Melbourne give appropriate consideration to whether large and high risk transactions should be processed.

g. On each occasion prior to August 2020 that senior management considered whether to continue the business relationship with Customer 38, senior management failed to give adequate consideration to whether the ML/TF risks posed by Customer 38 were within Crown Melbourne's risk appetite.

h. On each occasion prior to August 2021 that senior management considered whether to continue the business relationship with Customer 38, senior management failed to give adequate consideration to whether the ML/TF risks posed by Customer 38 were within Crown Perth's risk appetite.

Particulars

Section 36(1)(a) of the Act.

The due diligence steps taken with respect to Customer 38 included:

Database searches

In August 2019 and July 2020, Crown Melbourne performed risk intelligence and media searches.

None of these steps were proportionate to the ML/TF risks reasonably posed by Customer 38 on and from late 2016.

Senior management engagement

On 2 November 2018, following Crown's receipt of the email from a foreign bank, the AML Compliance Officer reviewed material from the Credit control team relating to Customer 38 including company searches, a credit check, the SYCO record of Customer 38's transactional activity, and his wins and losses at Crown Melbourne.

On 5 November 2018, Crown Perth assessed Customer 38's risk rating at the AML/CTF Compliance Officer Meeting and determined it would remain at moderate.

On 13 December 2018, Crown Melbourne reviewed documents held by the Credit control team relating to Customer 38 and his transaction history.

On 16 August 2019, the General Manager (AML) asked the AML Manager (Crown Melbourne) whether there was any material relevant to Customer 38 that would require an updated SMR to be given to the AUSTRAC CEO.

On 20 August 2019, the AML Manager (Crown Melbourne) responded, noting that he was of the view that there was no extra information that needed to be provided to AUSTRAC in the form of an SMR. He was of the view that the losses since the last SMR were within Customer 38's pattern.

At some time in August 2019, the General Manager (AML) began reviewing Customer 38's transactions in connection with a review of the Southbank accounts. She did not complete this work before leaving Crown. The work was not handed over and remained incomplete.

On the same day, the Chief Legal Officer (Australian Resorts) emailed the AML Manager (Crown Melbourne) regarding Customer 38 and asked whether there were any adverse reports relating to the customer. The AML Manager (Crown Melbourne) responded that there was no adverse media on Customer 38. He noted that the General Manager (AML) had started looking into him in August 2019 but did not complete that piece of work before she left Crown. No further action was taken following this email

None of these steps were proportionate to the ML/TF risks reasonably posed by Customer 38 on and from late 2016.

On 29 August 2020, Crown Melbourne issued an indefinite WOL in respect of Customer 38.

On 31 August 2021, Crown Perth issued an NRL in respect of Customer 38.

Enhanced customer due diligence

1600. Having formed a suspicion for the purposes of s41 of the Act, Crown Melbourne gave the AUSTRAC CEO SMRs with respect to Customer 38 on:

a. 19 April 2016;

b. 24 June 2016;

c. 15 September 2016;

d. 24 October 2016;

e. 31 October 2016;

f. 23 December 2016;

g. 4 January 2017;

h. 18 April 2017;

i. 23 June 2017;

j. 30 August 2017;

k. 9 January 2018;

l. 24 April 2018; and

m. 14 December 2018.

Particulars

Each of these SMRs reported threshold transactions, noted Customer 38's wins and losses and reported the amount of cash he was prepared to carry.

1601. Having formed a suspicion for the purposes of s41 of the Act, Crown Perth gave the AUSTRAC CEO an SMR with respect to Customer 38 on 5 May 2017.

Particulars

The SMR reported Customer 38's threshold transactions and transfers to third parties. It stated that Crown Melbourne believed that Customer 38 was using a third party, Person 51, as a money changer.

1602. On each occasion that Crown Melbourne and Perth formed a suspicion with respect to Customer 38 for the purposes of s41 of the Act, it was required to apply its ECDD program to Customer 38.

Particulars

Rule 15.9(3) of the Rules.

1603. Crown Melbourne and Crown Perth did not carry out appropriate risk-based ECDD measures with respect to Customer 38 on each occasion that Crown Melbourne and Crown Perth formed a suspicion with respect to Customer 38 for the purposes of s41 of the Act.

a. There are no records of ECDD being conducted following the lodgement of any SMRs save for the SMR dated 18 April 2017: see paragraphs 664 and 685.

b. Appropriate risk-based steps were not taken to obtain or analyse information about Customer 38's source of wealth/funds: see paragraph 667.

c. Appropriate risk-based steps were not taken to analyse and monitor Customer 38's transactions – both past and future – including to understand their economic purpose: see paragraphs 590 and 666.

d. On each occasion prior to August 2020 that senior management considered whether to continue the business relationship with Customer 38, senior management failed to give adequate consideration to whether the ML/TF risks posed by Customer 38 were within Crown Melbourne's risk appetite.

e. On each occasion prior to August 2021 that senior management considered whether to continue the business relationship with Customer 38, senior management failed to give adequate consideration to whether the ML/TF risks posed by Customer 38 were within Crown Perth's risk appetite: see paragraph 668ff.

Particulars

Rules 15.9(3), 15.10(1)(c), (d), (2), (5) and (6) of the Rules.

On 19 April 2017, Crown performed a company search for Company 11 and confirmed that Customer 38 was the company's only shareholder and director. Company records showed a foreign address for Customer 38, despite Crown Melbourne having a different foreign country address for him on their system.

See particulars to paragraph 1599.

1604. By reason of the matters pleaded from paragraphs 1585 to 1603, on and from late 2016, Crown Melbourne and Crown Perth:

a. did not monitor Customer 38 in relation to the provision of designated services, with a view to identifying, mitigating and managing the ML/TF risks reasonably faced; and

b. did not do so in accordance with rr 15.5 and 15.9 of the Rules.

1605. By reason of the matters pleaded at paragraph 1604, Crown Melbourne contravened s36(1) of the Act on and from late 2016 to 29 August 2020 with respect to Customer 38.

Particulars

Section 36(1) of the Act is a civil penalty provision: s36(2) of the Act.

1606. By reason of the matters pleaded at paragraph 1604, Crown Perth contravened s36(1) of the Act on and late 2016 to 31 August 2021 with respect to Customer 38.

Particulars

Section 36(1) of the Act is a civil penalty provision: s36(2) of the Act.

Customer 39

1607. Customer 39 was a customer of Crown Melbourne from 4 June 2007 to 30 July 2020 and a premium program player from 4 June 2007.

1608. From 4 June 2007 to 30 July 2020, Crown Melbourne provided Customer 39 with designated services within the meaning of table 1 and table 3, s6 of the Act.

Particulars

On 4 June 2007, Customer 39 registered at Crown Melbourne and was made a premium program player.

On 12 August 2012, Crown Melbourne opened a DAB account and a safekeeping account (AUD) for Customer 39.

On 6 December 2017, Crown Melbourne opened a CCF (AUD) for Customer 39 with a credit limit of $1,000,000. On 10 June 2021 Crown Melbourne closed the CCF (AUD) for Customer 39, by which time he had a line of credit up to $3,000,000.

As at 17 December 2020, Customer 39 had a total historical turnover of $1,369,795,545 and total historical losses of $22,456,618.

On 30 July 2020, Crown Melbourne issued an indefinite WOL in respect of Customer 39.

The ML/TF risks posed by Customer 39

1609. By 1 March 2016, higher ML/TF risks were indicated by the nature and purpose of Customer 39's business relationship with Crown Melbourne, the nature of the transactions he had been conducting, together with the suspicions Crown Melbourne itself had formed with respect to Customer 39.

Particulars

Section 36(1)(a), (b) of the Act and Chapter 15 of the Rules.

By 1 March 2016, Crown Melbourne had given the AUSTRAC CEO three SMRs in relation to Customer 39 – on 12 June 2013, 22 April 2015, and 28 January 2016. Each SMR reported the same patterns of suspicions relating to threshold transactions, telegraphic transfers received by Customer 39; a transfer of $300,000 from the DAB account of another customer, Customer 40, to Customer 39's account; the annual losses of Customer 39; and the amounts of cash Customer 39 was prepared to carry.

Collectively, the SMRs given to the AUSTRAC CEO by Crown Melbourne between 19 April 2010 and 10 July 2013 reported total wins of $1,324,100 and total losses of $126,900 over this 3 year period.

By at least 22 April 2015, Crown Melbourne was aware of an association between Customer 39 and Customer 40. By April 2015, Crown Melbourne was aware of large transfers of funds between the two customers.

1610. At all times in and from mid to late 2017, Customer 39 should have been recognised by Crown Melbourne as a high risk customer for the reasons pleaded at paragraphs 1609, 1612, 1613, 1614, 1615, 1616, 1617 and 1619.

Particulars

Section 36(1)(a), (b) of the Act and Chapter 15 of the Rules.

1611. It was not until 22 July 2020 that Customer 39 was rated high risk by Crown Melbourne.

Particulars

On various occasions between 11 June 2013 and 4 February 2019, Crown Melbourne assessed Customer 39's risk to be moderate, in spite of being aware of escalating high turnover on and from 2017 and lodging numerous SMRs.

On various occasions between 21 February 2019 and 20 July 2020, Crown Melbourne assessed Customer 39's risk to be significant.

Crown Melbourne did not assess Customer 39's risk as high until 22 July 2020, shortly before he was issued with a WOL.

See paragraph 120.

1612. On and from 1 March 2016 designated services provided to Customer 39 by Crown Melbourne posed higher ML/TF risks including because the provision of designated services to Customer 39 involved a combination of the following factors:

a. Customer 39 received high value financial (table 1, s6) and gaming services (table 3, s6);

b. by December 2020, Customer 39 had a total historical turnover of $1,369,795,545 and total historical losses of $22,456,618;

c. Crown Melbourne transferred large values of funds to and from Customer 39's bank accounts and his DAB account, involving designated services within the meaning of items 31 and 32, table 1, s6 of the Act: see paragraph 411ff;

d. Customer 39 regularly made transfers to or received transfers from third parties, including third parties in respect of whom Crown Melbourne had formed suspicions: see paragraph 456ff;

e. between August 2012 to April 2019, Customer 39 was recorded as either or both the remitter or the beneficiary in 121 transactions totalling $43,958,536;

f. on and from 2017, Customer 39's turnover escalated significantly;

g. on and from late 2017, designated services provided to Customer 39 involved patterns of unusual and large transactions involving third parties, cash and CVIs;

h. by early 2019, media reports named Customer 39 as a person involved in a proposal to acquire an interest in another Australian casino;

i. on and from 2019, Customer 39's turnover continued to escalate dramatically;

j. Customer 39 engaged in other transactions indicative of ML/TF typologies and vulnerabilities, including third party transactions: see paragraph 24;

k. Customer 39 carried and transacted using large amounts of cash and cash that appeared suspicious: see paragraphs 450, 451 and 452;

l. Crown Melbourne made available the Crown private jet for Customer 39. There were inadequate controls on the carrying of large amounts of cash on Crown's private jet: see paragraphs 454 and 491(c);

m. in early 2019, Customer 39 engaged in a number of suspicious cash transactions:

   i. in January 2019, Customer 39 presented at the Melbourne Cage with a large backpack with $300,000 in cash (all in $50 notes, with some of the funds wrapped in black plastic), which was deposited into his DAB account;

   ii. on 1 February 2019, Customer 39 presented $300,000 in cash from a shoebox at the Cage. Some of the notes were counterfeit;

n. in 2019, Crown Melbourne was advised that Customer 39 was of interest to law enforcement for a money laundering investigation;

o. on 17 July 2020, Crown Melbourne was served with a freezing order had been made against Customer 39 and his company, Company 5, in the NSW Supreme Court; and

p. by reason of the matters set out at subparagraphs a. to o. above, there were real risks that Customer 39's source of wealth and source of funds were not legitimate.

Monitoring of Customer 39's transactions

1613. At no time did Crown Melbourne appropriately monitor Customer 39's transactions on a risk-basis.

Particulars

Section 36(1)(a), (b) of the Act and Rules 15.4 to 15.8 of the Rules.

Crown Melbourne did not apply appropriate risk-based transaction monitoring to designated services provided to Customer 39: see paragraphs 590ff and 629 to 642.

Customer 39's transactions involved repeated transactions indicative of ML/TF typologies and vulnerabilities that were not detected prior to a 2021 lookback. Had appropriate risk-based transaction monitoring been applied, these transactions could have been identified earlier: see paragraphs 686 and 687.

Transactions indicative of ML/TF typologies – third party transfers

Transactions involving Customer 39 were identified as indicative of the ML/TF typology/typologies of third party transfers by an independent auditor in 2021.

From 10 February 2017 to 26 February 2020, 28 transactions were identified totalling $10,235,000 from third parties to a Southbank account for Customer 39.

Crown Melbourne's 2019 lookback

Sometime after April 2019, Crown prepared a list of transactions in which Customer 39 was recorded as either or both the remitter or the beneficiary from August 2012 to April 2019. There were 121 in total relating to Crown Melbourne totalling $43,958,536.

Crown Melbourne's 2021 lookback

On 24 August 2021, Crown Melbourne identified unusual historical activity by multiple Crown Rewards members, several of whom were associated with Customer 39. In particular:

- between December 2017 and February 2019, Person 37 received 18 direct transfers from Customer 39 to his Crown deposit account, totalling $1,350,000;
- between December 2017 and November 2018, Customer 39's brother received seven direct transfers from Customer 39 to his Crown deposit account, totalling $225,000;
- between November 2018 and February 2019, a Crown Melbourne patron received five direct transfers from Customer 39 to his Crown deposit account, totalling $325,000;
- on 9 November 2018, a Crown Melbourne patron received a direct transfer from Customer 39 to his DAB account of $25,000;
- between March 2016 and January 2019, Person 5 received seven direct transfers from Customer 39 to his DAB account, totalling $1,125,000; and
- between May 2017 and August 2017, Customer 39 received two direct transfers from Person 5 to his DAB account, totalling $325,000.

Inadequate controls on Crown's private jets

On 17 August 2016, Crown Melbourne made available the Crown private jet for Customer 39. The Crown private jet flew Customer 39, together with two other people, from the Sydney to Melbourne.

There were inadequate controls on the carrying of large amounts of cash on Crown's private jets: see paragraphs 454 and 491(c).

Ongoing customer due diligence

1614. On and from 2017, on multiple occasions, the provision of designated services to Customer 39 raised red flags reflective of higher ML/TF risks as a result of his escalating turnover and transactions with other Crown Melbourne patrons.

Particulars

See paragraphs 420ff and 456ff.

Large and unusual transactions and patterns of transactions in 2017

By the end of 2016, Customer 39's total losses for that year amounted to $1,425,533.

Customer 39's turnover and losses increased significantly from 2017.

By 10 February 2017, Customer 39's losses for 2017 to date amounted to $1,067,640. By 23 June 2017, Customer 39's losses for the year increased to $2,220,466 by June 2017 and $4,560,826 by

October 2017. By the end of the year Customer 39's total losses for 2017 amounted to $8,132,326.

On 14 December 2017, a telegraphic transfer in the amount of $1,000,000 was sent by Customer 40 and deposited in Customer 39's DAB account with Crown Melbourne.

Large and unusual transactions and patterns of transactions in 2018

Customer 39's turnover escalated during 2018. Customer 39's turnover for the 2018 financial year was $210,036,000 with losses of $7,954,000.

Reports prepared by Crown Melbourne in January and February 2018 showed Customer 39 had weekly turnover of up to around $50 million in these months.

On 5 February 2018, a second telegraphic transfer in the amount of $1,000,000 was sent by Customer 40 to Customer 39's DAB account.

By 6 February 2018, Customer 39's annual losses for 2018 to date amounted to $5,192,465. By June 2018, Customer 39's losses for the year had increased to $7,098,355. By November 2018, Customer 39's losses for the year were $6,668,620.

By November 2018, reports prepared by Crown Melbourne showed Customer 39 had weekly turnover of just under $125 million.

In November 2018, Customer 39 transferred a total of $875,000 from his DAB account (in 5 separate transactions) to the DAB account of 4 other customers including Customer 40.

Large and unusual transactions and patterns of transactions in 2019

Customer 39's turnover and losses continued to escalate from 2019.

For the 2019 financial year, Customer 39 had a turnover of $645,178,733 and losses of $7,686,550.

On 30 January 2019, Crown Melbourne produced a report which concerned Crown Melbourne highest turnover customers. The report noted that:

- Customer 39's turnover for the 2019 financial year to date was $482,080,000 with losses of $498,000; and
- Customer 39's turnover for the 2018 financial year was $210,036,000 with losses of $7,954,000.

By 30 January 2019, Customer 39's losses for 2019 to date amounted to $1,066,150. By 4 February 2019, Customer 39's losses for the year had increased to $7,240,500. By 22 March 2019, Customer 39's losses for the year had increased to $11,526,250.

On 25 January 2019, Customer 39 transferred $200,000 to the DAB account of Customer 40.

On 30 January 2019 Customer 39 made a further cash deposit of $130,000 into his DAB account.

By 4 February 2019, Customer 39's weekly turnover was $75,654,000 with losses of $4,853,000.

On 27 March 2019, a telegraphic transfer in the amount of AU$500,000 from Customer 40 was deposited in Customer 39's DAB account.

Large and unusual transactions and patterns of transactions in 2020

For the 2020 financial year, Customer 39 had a turnover of $4,257,000, losses of $774,950, and commission of $25,544 at Crown Melbourne. Customer 39 last received a designated service in that financial year on 5 March 2020, just before the COVID lockdowns.

Between 22 March 2019 and 5 March 2020, Customer 39 transferred $800,000 to his DAB account from his account with an Australian bank and he also received seven telegraphic transfers to his DAB account totalling $2,265,000 from an account with an Australian bank held in the name of Customer 40: SMR dated 7 May 2021.

1615. In 2019, on multiple occasions, the provision of designated services to Customer 39 raised red flags reflective of higher ML/TF risks as a result of large and suspicious cash transactions.

Particulars

See paragraphs 450 and 451.

At the same time that Customer 39's turnover for 2019 was continuing to escalate, Customer 39 was engaging in highly suspicious cash transactions.

On 23 January 2019, Customer 39 presented at Crown Melbourne a large backpack with $300,000 in cash (all in $50 notes, with some of the funds wrapped in black plastic) which were deposited into his DAB account. Crown Melbourne noted this conduct as unusual because Customer 39 was playing on a credit program and had not brought in such a significant amount before. No surveillance footage was available to detect the deposit of funds.

On 1 February 2019, Customer 39 presented a bag at the Cage which contained a shoe box full of cash, totalling $300,000, made up of $5,500 in $100 notes and $294,500 in $50 notes. The cash was presented in $5,000 and $10,000 lots bundled with rubber bands and did not appear to have been issued by a financial institution. Two of the $50 notes were discovered to be counterfeit. They were replaced by Customer 39 providing a $100 note. Customer 39 was asked about the origin of the funds, to which he replied that he had been given the funds by a friend and had brought the funds from Sydney. The funds were deposited and gaming chips issued to Customer 39.

1616. In 2019, on multiple occasions, the provision of designated services to Customer 39 raised red flags reflective of higher ML/TF risks as a result of receiving numerous enquiries from law enforcement agencies in respect of Customer 39.

Particulars

On 21 February 2019, Crown Melbourne received a law enforcement inquiry in respect of Customer 39.

On 22 March 2019, Crown Melbourne received a law enforcement inquiry in respect of Customer 39.

1617. In 2020, Crown Melbourne became aware of proceedings before the NSW Supreme Court relating to Customer 39's company.

Particulars

In July 2020, Crown Melbourne was served with a freezing order against Customer 39 and his company, Company 5, in the NSW Supreme Court.

By July 2020, Customer 39's companies were being put into voluntary administration and open sources reported that investors feared losses of more than $150 million.

In July 2020 open sources also reported on proceedings in the NSW Supreme Court, in which it was found that Customer 39 engaged in improper conduct and that the conduct of his companies had been dishonest and evasive; that Customer 39 regularly played in high-roller rooms at Crown Melbourne, and other Australian and overseas casinos.

1618. On and from mid to late 2017, Crown Melbourne failed to undertake appropriate risk-based customer due diligence with respect to Customer 39 with a view to identifying, mitigating and managing the ML/TF risks posed by the provision of designated services.

a. On and from mid to late 2017, Crown Melbourne was aware of unusual and suspicious transactional activity with respect to Customer 39, including escalating turnover and other transactions consistent with ML/TF typologies.

b. At no time did Crown Melbourne take appropriate steps to satisfy itself that Customer 39's source of wealth/funds were legitimate.

c. At no time did Crown Melbourne take appropriate steps to identify or analyse the ML/TF risks of Customer 39's transactions.

d. On each occasion prior to July 2020 that senior management considered whether to continue the business relationship with Customer 39, senior management failed to give adequate consideration to whether the ML/TF risks posed by Customer 39 were within Crown Melbourne's risk appetite.

Particulars

Section 36(1)(a) of the Act.

The due diligence steps taken with respect to Customer 39 included:

Wealth reports

In March 2019, Crown Melbourne obtained a wealth report for Customer 39 which placed him in a high wealth band.

Database searches

Between 18 and 24 September 2018, Crown Melbourne's VIP International team conducted various name, property, company and media searches in respect of Customer 39. It was not the purpose of these searches to assess the ML/TF risks of Customer 39.

In early February 2019, on becoming aware of Customer 39's presentation of counterfeit notes to the Cage, Crown Melbourne conducted various name, property, company and media searches in respect of Customer 39.

By the end of January 2019, Customer 39's turnover for the 2019 financial year to date was $482,080,000 with losses of $498,000. The due diligence conducted by Crown Melbourne in early 2019 did not adequately consider the ML/TF risks of this turnover by reference to his Customer 39's KYC information.

Crown Melbourne did not carry out any further ongoing due diligence with respect to Customer 39 until after it was served with the freezing order on 17 July 2020.

The 2017 due diligence profile

On 13 December 2017, Crown Melbourne produced a due diligence profile for Customer 39. It summarised various name, property, media and company searches conducted in respect of Customer 39 and identified his turnover. It identified that open source searches and wealth reports failed to provide any relevant details in respect of Customer 39.

These reviews did not have adequate regard to the ML/TF risks posed by Customer 39 on and from 1 March 2016.

Credit profiles

In around September 2019, Crown Melbourne produced a credit profile for Customer 39. The purpose of these searches was not to assess the ML/TF risks of Customer 39.

Senior management engagement

On 15 December 2017, the CTRM emailed the Head of Security and Surveillance attaching a document recording three transactions relating to Customer 39 on 14 December 2017. These transactions involved large amounts of cash and connections to third parties, including third parties in respect of whom Crown Melbourne had formed suspicions, namely Customer 40 and another Crown Melbourne patron:

On 22 March 2019, Customer 39 was added to the POI monitoring list.

At no time in 2019 did senior management give adequate consideration to the ML/TF risks posed by Customer 39 and whether an ongoing business relationship was within Crown Melbourne's ML/TF risk appetite.

On 20 July 2020, after being served with the freezing order in respect of Customer 39, the Chief Legal Officer of Crown Resorts and AML/CTF Compliance Officer for Crown Melbourne and Crown Perth was briefed with documents relating to Customer 39 including the wealth report and CURA extracts.

On 22 July 2020, recommendations were put to the POI Committee that stop codes be added to Customer 39's account and that he be issued with a WOL, on the basis that Crown would be exposed to a reputational risk if it continued to deal with Customer 39. Stop codes and comments were subsequently approved and applied.

On 30 July 2020, Crown Melbourne issued a WOL in respect of Customer 39.

The 2021 due diligence profile

In around January 2021, Crown Melbourne produced an updated Due Diligence Profile for Customer 39. The document:

- noted that Customer 39 had an outstanding debt of $680,515 to Crown Melbourne on a line of credit of $3,000,000;
- noted that Customer 39 was subject to a freezing order;
- under 'AML Check', noted the existence of adverse media concerning allegations against Customer 39 of being involved in the collapse of his companies, with investors expecting losses of more than $100,000,000, and that Customer 39 had been issued with a withdrawal of licence by the POI Committee due to reputational risk; and
- included a summary and copies of the searches obtained between 11 December 2020 and 21 January 2021.

In spite of the known ML/TF risks reasonably posed by Customer 39 from 2017, until July 2021, Crown Melbourne continued to pursue a business relationship with Customer 39 without appropriate consideration as to whether it was within risk appetite.

Enhanced customer due diligence

1619. Having formed a suspicion for the purposes of s41 of the Act, Crown Melbourne gave the AUSTRAC CEO SMRs with respect to Customer 39 on:

a. 18 October 2016;

b. 10 February 2017;

c. 23 June 2017;

d. 19 November 2017;

e. 15 December 2017;

f. 12 January 2018;

g. 6 February 2018;

h. 8 June 2018;

i. 9 November 2018;

j. 30 January 2019;

k. 4 February 2019;

l. 22 March 2019;

m. 7 May 2021; and

n. 24 August 2021.

Particulars

The SMRs reported on:

- Customer 39's annual losses;
- the amount of cash Customer 39 was prepared to carry; and
- Customer 39's telegraphic transfers with third parties.

1620. On each occasion that Crown Melbourne formed a suspicion with respect to Customer 39 for the purposes of s41 of the Act, it was required to apply its ECDD program to Customer 39.

Particulars

Rule 15.9(3) of the Rules.

1621. Crown Melbourne did not carry out appropriate risk-based ECDD measures with respect to Customer 39 on each occasion that Crown Melbourne formed a suspicion with respect to Customer 39 for the purposes of s41 of the Act.

a. There are no records of ECDD being conducted following the lodgement of any SMRs except for those given to the AUSTRAC CEO on 4 February 2019 and 22 March 2019: see paragraphs 664 and 685.

b. Appropriate risk-based steps were not taken to obtain or analyse information about Customer 39's source of wealth/funds: see paragraph 667.

c. Appropriate risk-based steps were not taken to analyse and monitor Customer 39's transactions – both past and future – including to understand their economic purpose: see paragraphs 590 and 666.

d. On each occasion prior to July 2020 that senior management considered whether to continue the business relationship with Customer 39, senior management failed to give adequate consideration to whether the ML/TF risks posed by Customer 39 were within Crown Melbourne's risk appetite: see paragraph 668ff.

e. In July 2020, after being served a freezing order relating to Customer 39, Crown Melbourne issued a WOL in respect of Customer 39.

Particulars

Rules 15.9(3), 15.10(1)(c), (d), (2), (5) and (6) of the Rules.

After lodging SMRs on 4 February 2019 and 22 March 2019, Crown Melbourne conducted various name, property, company and media searches in respect of Customer 39.

See particulars to paragraph 1618.

1622. By reason of the matters pleaded from paragraphs 1607 to 1621, on and from mid to late 2017, Crown Melbourne:

a. did not monitor Customer 39 in relation to the provision of designated services, with a view to identifying, mitigating and managing the ML/TF risks reasonably faced; and

b. did not do so in accordance with rr 15.5 and 15.9 of the Rules.

1623. By reason of the matters pleaded at paragraph 1622, Crown Melbourne contravened s36(1) of the Act on and from mid to late 2017 to 30 July 2020 with respect to Customer 39.

Particulars

Section 36(1) of the Act is a civil penalty provision: s36(2) of the Act.

Customer 40

1624. Customer 40 was a customer of Crown Melbourne from 1 February 2013 until 30 July 2020 and a premium program player from 6 February 2013.

1625. From at least 6 February 2013, Crown Melbourne provided Customer 40 with designated services within the meaning of table 1 and table 3, s6 of the Act.

Particulars

On 1 February 2013, Customer 40 registered at Crown Melbourne.

On 6 February 2013, Customer 40 was made a premium program player.

On 29 June 2013, Crown Melbourne opened a DAB account for Customer 40.

Between 2013 and 2015, Crown Melbourne recorded Customer 40's individual rated gaming activity to be a cumulative loss of $159,630.

In and from 2017, Customer 40's individual rated gaming activity escalated significantly. Between 2016 and November 2019, Crown Melbourne recorded Customer 40's individual rated gaming activity to be a cumulative buy-in of $25,485,800 with a loss of $10,668,656.

On 30 July 2020, Crown Melbourne issued a WOL in respect of Customer 40.

The ML/TF risks posed by Customer 40

1626. By 1 March 2016, higher ML/TF risks were indicated by the nature and purpose of Customer 40's business relationship with Crown Melbourne, the nature of the transactions he had been conducting, together with the suspicions Crown Melbourne itself had formed with respect to Customer 40.

Particulars

Section 36(1)(a), (b) of the Act and Chapter 15 of the Rules.

By 1 March 2016, Crown Melbourne had given the AUSTRAC CEO five SMRs in relation to Customer 40 – on 12 June 2013, 5 November 2014, 23 April 2015, 27 November 2015 and 28 January 2016. Each SMR reported suspicions based on annual losses and the amount of cash the customer was prepared to carry. In addition, the 27 November 2015 SMR noted a $75,000 transfer to Customer 40 from another Crown Melbourne customer, Person 12.

In 2013, Crown Melbourne recorded Customer 40's individual rated gaming activity to be a cumulative loss of $73,400.

In 2014, Crown Melbourne recorded Customer 40's individual rated gaming activity to be a cumulative loss of $86,543.

In 2015, Crown Melbourne recorded Customer 40's individual rated gaming activity to be a cumulative win of $313.

The 28 January 2016 SMR noted that on 25 January 2016, $300,000 was transferred from the DAB account of Customer 40 to the DAB account of Customer 39.

By 1 March 2016, Customer 40 was involved in 90 transactions to himself totalling approximately $11,945,165.

1627. At all times on and from 1 March 2016, Customer 40 should have been recognised by Crown Melbourne as a high risk customer by reason of the matters pleaded at paragraphs 1626, 1629, 1630, 1631 and 1633.

Particulars

Section 36(1)(a), (b) of the Act and Chapter 15 of the Rules.

1628. It was not until 19 July 2020 that Customer 40 was rated high risk by Crown Melbourne.

Particulars

Crown Melbourne did not assess Customer 40 as high risk until after it became aware of a media report on 19 July 2020 regarding Customer 40's connection to Customer 39 and a company, Company 5, which was subject to a freezing order made in the NSW Supreme Court.

See paragraph 120.

1629. On and from 1 March 2016 designated services provided to Customer 40 posed higher ML/TF risks, including because the provision of designated services to Customer 40 involved a combination of the following factors:

a. Customer 40 received high value financial (table 1, s6) and gaming services (table 3, s6);

b. by November 2019, Crown Melbourne recorded Customer 40's individual rated gaming activity to be a cumulative loss of $10,668,656;

c. Customer 40 carried large amounts of cash and transacted using large amounts of cash and cash that appeared suspicious: see paragraphs 450, 451 and 452;

d. Crown Melbourne transferred large values to and from Customer 40's bank accounts and his DAB account, involving the provision by Crown Melbourne of designated services within the meaning of items 31 and 32, table 1, s6 of the Act: see paragraph 411ff;

e. Customer 40 regularly made transfers to or received transfers from third parties, including individuals associated with the Meg-Star and Suncity junkets in respect of whom Crown Melbourne had formed suspicions: see paragraph 456ff;

f. Customer 40 engaged in other transactions indicative of ML/TF typologies and vulnerabilities, including the use of third party agents: see paragraph 24;

g. from at least January 2016, Crown Melbourne was aware that Customer 40 was connected to Customer 39, a person in respect of whom Crown Melbourne had formed suspicions;

h. on and from 2017, Customer 40's turnover escalated significantly;

i. on and from 2017, designated services provided to Customer 40 involved patterns of unusual and large transactions involving third parties;

j. between 1 March 2016 and 26 February 2020, Customer 40 engaged in over 116 telegraphic transfers totaling $62,094,465;

k. these transactions took place against the background of:

   i. by 1 March 2016, Customer 40 was involved in 90 transactions to himself totalling approximately $11,945,165; and

   ii. five SMRs being given to the AUSTRAC CEO by Crown Melbourne by 1 March 2016;

l. by reason of the matters set out at subparagraphs a. to k. above, there were higher ML/TF risks associated with Customer 40's source of wealth/funds

Monitoring of Customer 40's transactions

1630. At no time did Crown Melbourne appropriately monitor Customer 40's transactions on a risk-basis.

Particulars

Section 36(1)(a), (b) of the Act and Rules 15.4 to 15.8 of the Rules.

Crown Melbourne did not apply appropriate risk-based transaction monitoring to designated services provided to Customer 40: see paragraphs 590ff and 629 to 642.

Customer 40's transactions involved repeated transactions indicative of ML/TF typologies and vulnerabilities that were not detected prior to a 2021 lookback. Had appropriate risk-based transaction monitoring been applied, these transactions could have been identified earlier: see paragraphs 686 and 687.

Large and suspicious transactions – suspicion of involvement with other criminal activities

An independent auditor in 2021 identified Customer 40 as a beneficiary suspected of involvement in other criminal activity and noted a transfer of $600,000 from the Meg-Star junket operator, Customer 3 to Customer 40 on 16 April 2019.

Transactions indicative of ML/TF typologies – use of third party agents

Transactions involving Customer 40 were identified as indicative of the ML/TF typology of the use of third party agents by an independent auditor in 2021.

On 16 August 2016, Customer 40 received a telegraphic transfers of $300,000 from a third party company. The transaction description also referred to Customer 22.

The independent auditor also identified a number of transactions indicative of the ML/TF typology of the use of third party agents in which the transaction narrative referred to Customer 40, but which were made to patrons with no apparent connection to Customer 40:

- On 20 and 21 May 2017, two transfers of $20,000 each were made to a Crown Melbourne patron with the transaction narrative indicating that the transfer was from Customer 40, and for or connected with Customer 39.
- On 26 September 2017, a transfer of $57,529 was made to a Crown Melbourne patron with the transaction narrative indicating that the transfer was from Customer 40, and for or connected with Customer 39.
- On 14 January 2020, a transfer of $25,000 was made to a Crown Melbourne patron with the transaction narrative indicating that the transfer was from Customer 40, and for or connected with Customer 39.
- On 21 February 2020, a transfer of $331,000 was made to a Crown Melbourne patron with the transaction narrative indicating that the transfer was from Customer 40, and for or connected with Customer 39.

Crown Melbourne's 2020 lookback

Sometime after March 2020, Crown prepared a list of transactions in which Customer 40 was recorded as either the remitter or the beneficiary of telegraphic transfers from 1 March 2016 to 26 February 2020. There were over 116 telegraphic transfers relating to Customer 40 at Crown Melbourne totaling $62,094,465, including:

- on 14 December 2017, Customer 40 transferred $1,000,000 to Customer 39;

- on 21 December 2017, Customer 40 transferred $1,000,000 to Customer 39;
- on 25 January 2018, Customer 40 transferred $2,000,000 to Customer 39 through two $1,000,000 transactions;
- on 5 February 2018, Customer 40 transferred $1,000,000 to Customer 39;
- on 18 March 2018, Customer 40 transferred $1,170,226 between his accounts;
- on 8 November 2018, Customer 40 transferred $2,000,000 between his accounts;
- on 2 December 2018, Customer 40 transferred $1,723,873 between his accounts;
- on 27 January 2019, Customer 40 transferred $1,000,000 to himself;
- on 29 January 2019, Customer 40 transferred $1,000,000 to himself;
- on 31 January 2019, Customer 40 transferred $2,000,000 to himself;
- on 2 February 2019, Customer 40 transferred $1,000,000 to himself; and
- on 8 February 2019, Customer 40 transferred $2,000,000 to himself.

Crown Melbourne's 2021 lookback

Customer 40's transactions involved repeated transactions indicative of ML/TF typologies that were not detected prior to a 2021 look-back. On 24 August 2021, Crown Melbourne identified unusual historical activity by multiple Crown rewards members who were associated with Customer 40, including Customer 39. In particular, the lookback for Customer 40 noted:

- on 26 November 2015, a Crown Melbourne patron, Person 12, made a direct transfer of $75,000 to Customer 40;
- between February 2016 and August 2017, Customer 40 sent a Crown Melbourne patron, Person 5, eight direct transfers totalling $775,000;
- between December 2017 and March 2019, Customer 40 sent a Crown Melbourne patron, Person 5, two direct transfers totalling $300,000;
- on 16 March 2018, Customer 40 transferred $75,000 to a Crown Melbourne patron, Person 37;

- on 22 March 2019, Crown Melbourne received a telegraphic transfer for a Crown Melbourne patron, Person 5, sent by Customer 40 from an Australian bank account; and
- on 19 September 2019, Customer 40 sent a telegraphic transfer in the amount of $500,000 from his account with an Australian bank to a Crown Melbourne patron, Person 12's, DAB account.

Ongoing customer due diligence

1631. On and from 1 March 2016 on multiple occasions, the provision of designated services to Customer 40 raised red flags reflective of higher ML/TF risks.

Particulars

See paragraphs 450, 451 and 456ff.

Escalating play

Between 2016 and 2018, Customer 40's play increased significantly. His average bet almost doubled over this time:

- in 2016, Crown Melbourne recorded Customer 40's individual rated gaming activity to be a total buy-in of $7,514,000 with a loss of $498,268. His average bet was $12,569;
- in 2017, Crown Melbourne recorded Customer 40's individual rated gaming activity to be a total buy-in of $9,675,800 with a loss of $5,659,885. His average bet was $21,474; and
- in 2018, Crown Melbourne recorded Customer 40's individual rated gaming activity to be a total buy-in of $6,261,500 with a loss of $3,629,199. His average bet was $22,379.

Large or unusual transactions

During the following times, designated services provided to Customer 40 involved complex, unusual large transactions and unusual patterns of transactions which had no apparent economic or visible lawful purpose:

- on 5 February 2017, Crown Melbourne exchanged $72,095 in gaming chips to cash for Customer 40. Crown Melbourne noted that the value of chips exchanged did not reflect Customer 40's rated gaming play: SMR dated 6 February 2017;
- on 9 February 2017, Crown Melbourne recorded that Customer 40 transferred $500,000, $300,000, $150,000 and $466,356 between his accounts;
- on 26 June 2017, Crown Melbourne recorded that Customer 40 transferred $75,000 to Customer 39;
- on 8 November 2017, Customer 40 withdrew $98,000 in cash from his DAB account;
- on 14 December 2017, Customer 40 ordered a telegraphic transfer of $1,000,000 for Customer 39;

- on 5 February 2018, Crown Melbourne received a telegraphic transfer of $1,000,000 ordered by Customer 40, for the DAB account of Customer 39;
- on 9 November 2018, Customer 39 transferred $500,000 from his DAB account to Customer 40's DAB account;
- on 11 November 2018, Customer 40 transferred $300,000 into his DAB account; and
- in November 2018, Customer 40 received two $50,000 telegraphic transfers from a third party.

Ongoing table 1, s6 designated services

Crown Melbourne last provided Customer 40 with a table 3, s6 designated service on 11 March 2019. However, Crown Melbourne continued to receive and process funds transferred by Customer 40 to other customers at Crown Melbourne:

- on 22 March 2019, Crown received a bank transfer of $100,000 from Customer 40 for a Crown Melbourne patron, Person 5;
- on 27 March 2019, Customer 40 sent a telegraphic transfer of $500,000 to Customer 39's DAB account;
- on 9 April 2019, Crown Melbourne received a telegraphic transfer of $600,000 for Customer 3, ordered by Customer 40;
- on 19 September 2019, Crown Melbourne received a telegraphic transfer of $500,000 for a Crown Melbourne patron, Person 12, which was ordered by Customer 40;
- on 2 October 2019, Crown Melbourne received a telegraphic transfer of $300,000 for Customer 3, ordered by Customer 40; and
- on 25 November 2019, Crown Melbourne received a telegraphic transfer of $250,000 for the Meg-Star junket operator, Customer 3, ordered by Customer 40.

On 26 July 2020, Customer 40 is alleged to have fled Australia.

On 30 July 2020, Crown Melbourne issued a WOL in respect of Customer 40.

1632. At no time did Crown Melbourne undertake appropriate risk-based customer due diligence with respect to Customer 40 with a view to identifying, mitigating and managing the ML/TF risks posed by the provision of designated services on and from 1 March 2016.

a. At no time did Crown Melbourne take appropriate steps to understand whether Customer 40's source of wealth/funds was legitimate.

b. At no time did Crown Melbourne take appropriate steps to identify or analyse the ML/TF risks of Customer 40's transactions or to consider whether they had a lawful purpose.

c. At no time did Crown Melbourne give appropriate consideration to whether large and high risk transactions should be processed.

d. Prior to the decision to issue Customer 40 with a WOL in July 2020, there is no record of senior management considering whether continuing the business relationship with Customer 40 was within Crown Melbourne's ML/TF risk appetite in light of the ML/TF risks posed by Customer 40.

Particulars

Section 36(1)(a) of the Act.

The due diligence steps taken with respect to Customer 40 included:

Prior to May 2020, Crown Melbourne conducted two company searches in respect of a company associated with Customer 40 in 2019 and a media search for the same company. Customer 40 was not a director of the company at the time the searches were carried out.

In May 2020, two companies that Customer 40 was director of were the defendants in a hearing in the Supreme Court of New South Wales. Judgment was entered in favour of the plaintiffs comprising a large sum.

By July 2020, Customer 39's companies, with which Customer 40 was associated, were in the process of being put into voluntary administration and open sources reported that investors feared losses of more than $150 million.

On 23 July 2020, Customer 40 was escalated to the POI Committee following an adverse media report. Stop codes were applied to Customer 40's account.

On 30 July 2020, Crown Melbourne issued a WOL in respect of Customer 40.

On 14 August 2020, Customer 40 was mentioned in a media article which described him as an executive officer of Customer 39's company, Company 5, which owed creditors $350 million. The article described Customer 40 and Customer 39 as running a "crude Ponzi scheme".

Enhanced customer due diligence

1633. Having formed a suspicion for the purposes of s41 of the Act, Crown Melbourne gave the AUSTRAC CEO SMRs with respect to Customer 40 on:

a. 6 February 2017;

b. 10 February 2017;

c. 23 June 2017;

d. 9 November 2017;

e. 15 December 2017;

f. 6 February 2018;

g. 12 November 2018;

h. 21 November 2018;

i. 22 March 2019;

j. 10 April 2019;

k. 20 September 2019;

l. 3 October 2019;

m. 26 November 2019;

n. 7 May 2021; and

o. 24 August 2021.

Particulars

The SMRs reported:

- Customer 40's annual losses;
- Customer 40's exchange of chips to cash in amounts that did not reflect his play;
- the amount of cash Customer 40 was prepared to carry; and
- Customer 40's threshold transactions and telegraphic transfers with third parties.

1634. On each occasion that Crown Melbourne formed a suspicion with respect to Customer 40 for the purposes of s41 of the Act, it was required to apply its ECDD program to Customer 40.

Particulars

Rule 15.9(3) of the Rules.

1635. Crown Melbourne did not carry out appropriate risk-based ECDD measures with respect to Customer 40 on each occasion that Crown Melbourne formed a suspicion with respect to Customer 40 for the purposes of s41 of the Act.

a. There are no records of ECDD being conducted following the lodgement of any of the SMRs given to the AUSTRAC CEO between 6 February 2017 and 24 August 2021: see paragraphs 664 and 685.

b. Appropriate risk-based steps were not taken to obtain or analyse information about Customer 40's source of wealth/funds: see paragraph 667.

c. Appropriate risk-based steps were not taken to analyse and monitor Customer 40's transactions – both past and future – including to understand their economic purpose: see paragraphs 590 and 666.

d. Prior to the decision to issue Customer 40 with a WOL in July 2020, there is no record of senior management considering whether continuing the business relationship with Customer 40 was within Crown Melbourne's ML/TF risk appetite in light of the ML/TF risks posed by Customer 40: see paragraph 668ff.

Particulars

Rules 15.9(3), 15.10(1)(c), (d), (2), (5) and (6) of the Rules.

See particulars to paragraph 1632.

1636. By reason of the matters pleaded from paragraphs 1624 to 1635, on and from 1 March 2016, Crown Melbourne:

a. did not monitor Customer 40 in relation to the provision of designated services, with a view to identifying, mitigating and managing the ML/TF risks reasonably faced; and

b. did not do so in accordance with rr 15.5 and 15.9 of the Rules.

1637. By reason of the matters pleaded at paragraph 1636, Crown Melbourne contravened s36(1) of the Act on and from 1 March 2016 to July 2020 with respect to Customer 40.

Particulars

Section 36(1) of the Act is a civil penalty provision: s36(2) of the Act.

Customer 41

1638. Customer 41 has been a customer of Crown Melbourne since at least 14 July 2012.

1639. From at least 14 July 2012, Crown Melbourne provided Customer 41 with designated services within the meaning of table 1 and table 3, s6 of the Act.

Particulars

On 16 September 2013, Crown Melbourne opened a DAB account and a safekeeping account (AUD) for Customer 41.

On 22 September 2017, Crown Melbourne opened a Card Play Extra account (AUD) for Customer 41.

Customer 41 was a Premium Program player.

Between 2012 and 2015, Crown Melbourne recorded Customer 41's individual rated gaming activity to be a cumulative turnover of $99,906,691, a cumulative buy-in of $3,106,500 with a cumulative loss of $7,400,110.

Between 2016 and 2020, Crown Melbourne recorded Customer 41's individual rated gaming activity to be a cumulative turnover of $656,584,848 with a cumulative loss of $75,252,044.

The ML/TF risks posed by Customer 41

1640. By 1 March 2016, higher ML/TF risks were indicated by the nature and purpose of Customer 41's business relationship with Crown Melbourne, the nature of the transactions she had been conducting, together with the suspicions Crown Melbourne itself had formed with respect to Customer 41.

Particulars

Section 36(1)(a), (b) of the Act and Chapter 15 of the Rules.

SMRs by 1 March 2016

Between 17 September 2013 and 11 August 2015, Crown Melbourne gave the AUSTRAC CEO seven SMRs in relation to Customer 41 – on 17 September 2013, 8 October 2013, 17 October 2013, 9 May 2014, 7 October 2014, 4 March 2015, and 11 August 2015. Each

SMR reported the same patterns of suspicions relating to the annual rated gaming activity of Customer 41, Customer 41's association with another patron who was also known to be Customer 41's husband and the amounts of cash Customer 41 was prepared to carry.

Collectively, the SMRs given to the AUSTRAC CEO between 17 September 2013 and 11 August 2015 reported for Customer 41 total losses of $5,476,937 over this two year period.

Individual rated gaming activity by 1 March 2016

In 2012, Crown Melbourne recorded Customer 41's individual rated gaming activity as a turnover of $164,827.45, with a buy-in of $0 and losses of $24,300.56.

In 2013, Crown Melbourne recorded Customer 41's individual rated gaming activity as a turnover of $11,633,095.65, with a buy-in of $5,000 and losses of $979,594.03.

In 2014, Crown Melbourne recorded Customer 41's individual rated gaming activity as a turnover of $34,887,326, with a buy-in of $201,500 and losses of $2,142,164.61.

In 2015, Crown Melbourne recorded Customer 41's individual rated gaming activity as a turnover of $53,221,442.10, with a buy-in of $2,900,000 and losses of $4,254,051.

Law enforcement enquiries in 2015

In August and October 2015, Crown Melbourne received law enforcement inquiries regarding Customer 41 and her husband relating to a money laundering investigation and theft of foreign currency: SMR dated 26 March 2021.

1641. As at 1 March 2016, Customer 41 should have been recognised by Crown Melbourne as a high risk customer for the reasons pleaded at paragraph 1640.

1642. It was not until 26 March 2021 that Customer 41 was rated high risk by Crown Melbourne.

Particulars

On various occasions between 17 September 2013 and 23 January 2017, Crown Melbourne assessed Customer 41 as moderate risk.

On various occasions between 26 August 2015 and 1 November 2019, Crown Melbourne assessed Customer 41 as significant risk.

This was despite Customer 41's significant individual rated gaming activity by 1 March 2016 and the two law enforcement enquiries made in respect of Customer 41 and her husband in connection with money laundering and the theft of foreign currency.

On 26 March 2021, Customer 41 was rated high risk by Crown Melbourne.

See paragraph 120.

1643. At all times on and from 1 March 2016, Customer 41 should have been recognised by Crown Melbourne as a high risk customer by reason of the matters pleaded at paragraphs 1640, 1644, 1645, 1646, 1647, 1648 and 1650.

Particulars

Section 36(1)(a), (b) of the Act and Chapter 15 of the Rules.

1644. On and from 1 March 2016 designated services provided to Customer 41 posed higher ML/TF risks including because the provision of designated services to Customer 41 involved a combination of the following factors:

a. the table 3, s6, designated services provided to Customer 41 involved escalating rates of high turnover;

b. by 2020, Crown Melbourne recorded Customer 41's individual rated gaming activity to be a cumulative turnover of $756,491,539 with a cumulative loss of $81,672,557;

c. between 2013 and 2020, Customer 41 deposited 59 bank cheques totalling $13,518,075;

d. designated services provided to Customer 41 involved large transfers to and from third parties, including to and from other junket operators, foreign remittance service providers and unknown third parties: see paragraph 456ff;

e. designated services provided to Customer 41 involved large cross-border movements of funds, including through the Southbank accounts: see paragraph 239;

f. large values of funds were transferred to and from Customer 41's bank accounts and her DAB account, and to and from other customers' DAB accounts, involving designated services within the meaning of items 31 and 32, table 1, s6 of the Act;

g. Customer 41 carried large amounts of cash and transacted using large amounts of cash;

h. Customer 41 frequently received cancel credits from EGM play, which is indicative of the ML/TF typology/vulnerability of quick turnover of funds (without betting);

i. Customer 41 engaged in other transactions indicative of ML/TF typologies and vulnerabilities, including use of third party agents: see paragraph 24;

j. these transactions took place against the background of law enforcement having expressed an interest in Customer 41 in 2015 in relation to a money laundering investigation;

k. by 11 March 2016, Customer 41 had transacted $3,050,000 through Crown Towers Hotel for redemption at Crown Melbourne during FY2016: see paragraphs 244, 418, 419 and 650; and

l. by reason of the matters set out at subparagraphs a. to k. above, there were real risks that Customer 41's source of wealth and source of funds were not legitimate.

Monitoring of Customer 41's transactions

1645. At no time did Crown Melbourne appropriately monitor Customer 41's transactions on a risk-basis.

Particulars

Section 36(1)(a), (b) of the Act and Rules 15.4 to 15.8 of the Rules.

Crown Melbourne did not apply appropriate risk-based transaction monitoring to designated services provided to Customer 41: see paragraphs 590ff and 629 to 642.

Customer 41's transactions involved repeated transactions indicative of ML/TF typologies and vulnerabilities that were not detected prior to a 2021 look-back. Had appropriate risk-based transaction monitoring been applied, these transactions could have been identified earlier: see paragraphs 686 and 687.

The March 2021 Crown Melbourne lookback

The 2021 Crown Melbourne lookback (SMR dated 26 March 2021) identified that:

- Customer 41 had made the following foreign exchange transactions:
  - on 24 May 2018 Customer 41 exchanged a large amount in a foreign currency;
  - between 1 April 2019 and 11 March 2020 Customer 41 exchanged a large sum in a foreign currency in 9 separate transactions;
  - on 31 August 2019 Customer 41 exchanged a large amount in a foreign currency;
- between 2013 and 2020 Customer 41 had deposited 59 bank cheques totalling $13,518,075;
- Customer 41 had been linked to the following telegraphic transfers:
  - on 6 February 2015 a telegraphic transfer of AU$70,733 in a foreign currency was sent by Customer 41 to a third party;
  - on 18 October 2018 a telegraphic transfer of $600,000 was received by Customer 41 from a third party account in a foreign country;
  - on 2 November 2018, a telegraphic transfer of $800,000 was received by Customer 41 from a third party account in a foreign country;
  - on 5 April 2019 a telegraphic transfer of $500,000 was sent to Customer 41 from an overseas account in a foreign country held in Customer 41's name, with reference to gaming;
  - on 1 March 2019 a telegraphic transfer of $800,000 was sent to Customer 41 from a foreign bank account in a foreign country held in Customer 41's name, with reference to gaming;

- on 21 October 2019 and 10 February 2020, Customer 41 received telegraphic transfers of $523,879 and $850,000 from a third party Australian bank account; and

- between 23 September 2015 and 3 March 2017 Customer 41 conducted 9 telegraphic transfers totalling approximately $2,635,147 over 9 transactions to an Australian bank account in Customer 41's name.

Transactions indicative of ML/TF typologies – use of third party agents

Transactions involving Customer 41 were identified as indicative of the ML/TF typology of use of third party agents by an independent auditor in 2020 and 2021. The transactions totalled $3,573,828:

- on 17 October 2018, a deposit of $599,993 was made into a Southbank account. Crown Melbourne matched this deposit to Customer 41. The third party sender was identified as a foreign remittance company;

- on 1 November 2018, a deposit of $799,993 was made into a Southbank account with a transaction narrative that included the name of another Crown Melbourne customer, Customer 22. Crown Melbourne matched this deposit to Customer 41. The third party sender was identified as a foreign remittance company;

- on 22 February 2019, a deposit of $799,993 was made into a Southbank account with a transaction narrative that included the name of another Crown Melbourne customer, Customer 22. Crown Melbourne matched this deposit to Customer 41. The third party sender was identified as a company;

- on 21 October 2019, a deposit of $523,849 was made into a Crown Melbourne Limited account. Crown Melbourne matched this deposit to Customer 41. The third party sender was identified as an individual and a patron;

- on 10 February 2020, a deposit of $850,000 was made into a Crown Melbourne account. Crown Melbourne matched this deposit to Customer 41. The third party sender was identified as an individual and a patron.

Ongoing customer due diligence

1646. On and from 1 March 2016, on multiple occasions, the provision of designated services to Customer 41 by Crown Melbourne raised red flags reflective of higher ML/TF risks as a result of her use of the HCT channel.

Particulars

See paragraphs 418, 419, 420 and 422.

Crown Melbourne engaged in a practice in which it would receive payment at Crown Towers Hotel from international VIP customers using a credit or debit card (ordinarily a foreign credit card). The

funds were then made available to the customer for gaming at Crown Melbourne.

By 11 March 2016, Customer 41 had transferred $3,050,000 through the HCT channel in FY2016: see paragraphs 244, 418, 419 and 650.

1647. On and from 1 March 2016, on multiple occasions, the provision of designated services to Customer 41 by Crown Melbourne raised red flags reflective of higher ML/TF risks as a result of her frequent, large transactions that often involved third parties.

Particulars

See paragraph 420ff and 456ff.

During the following times, designated services provided to Customer 41 involved complex, unusual large transactions and unusual patterns of transactions which had no apparent economic or visible lawful purpose:

Large and suspicious transactions and patterns of transactions in 2016

In 2016, Crown Melbourne recorded Customer 41's individual rated gaming activity to be a turnover of $136,507,602 with losses of $14,345,783.

On 14 July 2016, Customer 41 received three deposits totalling $300,000 into her DAB account. Each transfer had the descriptor "BANK TRANSACTION".

On 15 October 2016, $300,000 was deposited into Customer 41's DAB account with the descriptor "PRE APPROVED BANK TRANSACTION".

Large and suspicious transactions and patterns of transactions in 2017

In 2017, Crown Melbourne recorded Customer 41's individual rated gaming activity to be a turnover of $136,979,842 with losses of $13,905,151.24 at Crown Melbourne.

On 24 August 2017, Customer 41 received a transfer of $500,000 to her DAB account. On the same day, she transferred $500,000 to another Crown Melbourne customer's DAB account: SMR dated 28 August 2017.

Large and suspicious transactions and patterns of transactions in 2018

In 2018, Crown Melbourne recorded Customer 41's individual rated gaming activity to be a turnover of $122,308,040 with losses of $16,267,436.33 at Crown Melbourne.

On 12 October 2018, Customer 41 received a $1,000,000 transfer to her DAB account from the DAB account of another Crown Melbourne customer: SMR dated 15 October 2018. Crown Melbourne believed that the third party was Customer 41's assistant.

On 18 October 2018 and 2 November 2018, Customer 41 received a telegraphic transfer in the amount of $600,000 and $800,000 respectively from a third party: SMRs dated 19 October 2018 and 7 November 2018.

Large and suspicious transactions and patterns of transactions in 2019

In 2019, Crown Melbourne recorded Customer 41's individual rated gaming activity to be a turnover of $208,649,254 with losses of $27,512,150 at Crown Melbourne.

Large and suspicious transactions and patterns of transactions in 2020

In 2020, Crown Melbourne recorded Customer 41's individual rated gaming activity to be a turnover of $52,140,107.40, with a buy-in of $0 and losses of $3,221,522.44 at Crown Melbourne.

1648. On and from 1 March 2016, on multiple occasions, the provision of designated services to Customer 41 by Crown Melbourne raised red flags reflective of higher ML/TF risks as a result of her gaming activity, which involved transactions with large amounts of cash.

Particulars

See paragraph 435.

On 14 July 2016, Customer 41 took a total of $29,264 in gaming machine jackpots in cash. Customer 41 deposited the same amount into her DAB account on the same day.

Between 23 and 26 September 2016, Crown Melbourne recorded:

- Gaming Machine Cancel Credits for Customer 41 credited as $96,594 in cash and $700,234 to her DAB account;
- Gaming Machine Jackpots for Customer 41 credited as $27,585 in cash and $150,000 to her DAB account;
- a machine payout of $11,878; and
- cash withdrawals by Customer 41 from her DAB account totalling $51,876.

On 27 September 2016, Customer 41 withdrew $140,000 from her DAB account in two separate transactions with the descriptor "TO CASHLESS". On the same day, Customer 41 deposited $10,770 and withdrew a further $180,000.

Between 14 to 16 October 2016, Crown Melbourne recorded:

- Gaming Machine Cancel Credits for Customer 41 credited as $12,551 in cash, $110,000 by cheque and $160,000 to her DAB account;
- Gaming Machine Jackpots for Customer 41 credited as $58,734 in cash and $100,000 to her DAB account;
- Machine payouts totalling $98,839;

- cash withdrawals by Customer 41 from her DAB account totalling $129,358; and
- a cash deposit into Customer 41's DAB account of $16,710.30.

1649. At no time did Crown Melbourne undertake appropriate risk-based customer due diligence with respect to Customer 41 with a view to identifying, mitigating and managing the ML/TF risks posed by the provision of designated services on and from 1 March 2016.

a. At no time did Crown Melbourne take appropriate steps to understand Customer 41's source of wealth/funds was legitimate.

b. At no time did Crown Melbourne take appropriate steps to identify or analyse the ML/TF risks of Customer 41's transactions or to consider whether they had a lawful purpose.

c. At no time did Crown Melbourne take appropriate steps to understand the relationship between Customer 41 and the third parties to whom she was transferring funds, or from whom she was receiving transfers of funds.

d. At no time did Crown Melbourne give appropriate consideration to whether large and high risk transactions should be processed.

e. At no time did senior management consider whether continuing the business relationship with Customer 41 was within Crown Melbourne's ML/TF risk appetite.

Particulars

Section 36(1)(a) of the Act.

Crown Melbourne carried out ECDD in respect of Customer 41 in January 2018: see particulars to paragraph 1652. Otherwise, Crown Melbourne did not carry out any due diligence in respect of Customer 41 until December 2020. This was despite that, by 2020, Crown Melbourne recorded Customer 41's individual rated gaming activity to be a cumulative turnover of $756,491,539.

Between 10 December 2020 and 16 February 2021, Crown Melbourne conducted company, land title and open source searches and obtained a risk intelligence report relating to Customer 41. The report estimated Customer 41 to be high net worth and identified her association with Australia-based and international companies.

On 16 November 2021, the Group Senior Manager, Financial Crime Investigations & Screening emailed a Financial Crime Analyst stating he wanted to finalise the senior management acceptance for Customer 41 because she was due to travel to Australia in early 2022. No conclusion was reached.

None of these steps were proportionate to the ML/TF risks reasonably posed by Customer 41 on and from 1 March 2016.

Enhanced customer due diligence

1650. Having formed a suspicion for the purposes of s41 of the Act, Crown Melbourne gave the AUSTRAC CEO SMRs with respect to Customer 41 on:

a. 5 May 2016;

b. 15 July 2016;

c. 27 September 2016;

d. 17 October 2016;

e. 13 July 2017;

f. 28 August 2017;

g. 24 January 2018;

h. 15 October 2018;

i. 19 October 2018;

j. 7 November 2018;

k. 1 November 2019; and

l. 26 March 2021.

Particulars

Each of these SMRs reported suspicions based on Customer 41's annual losses and the amounts of cash she was prepared to carry.

1651. On each occasion that Crown Melbourne formed a suspicion with respect to Customer 41 for the purposes of s41 of the Act, it was required to apply its ECDD program to Customer 41.

Particulars

Rule 15.9(3) of the Rules.

1652. Crown Melbourne did not carry out appropriate risk-based ECDD measures with respect to Customer 41 on each occasion that Crown Melbourne formed a suspicion with respect to Customer 41 for the purposes of s41 of the Act.

a. Other than in January 2018, there are no records of ECDD being conducted following the lodgement of any SMRs: see paragraphs 666.

b. Appropriate risk-based steps were not taken to obtain or analyse information about Customer 41's source of wealth/funds: see paragraph 667.

c. Appropriate risk-based steps were not taken to analyse and monitor Customer 41's transactions – both past and future – including to understand their economic purpose: see paragraphs 590 and 666.

d. At no time did senior management consider whether continuing the business relationship with Customer 41 was within Crown Melbourne's ML/TF risk appetite: see paragraph 668ff.

Particulars

Rules 15.9(3), 15.10(1)(c), (d), (2), (5) and (6) of the Rules.

After lodging the SMR on 24 January 2018, Crown Melbourne conducted a number of database searches for Customer 41 including a company search and a risk intelligence search. Crown Melbourne also requested a wealth report but was advised that no information had been located on Customer 41. The response regarding the

wealth report request was forwarded to the CTRM and the Group General Manager (AML).

On 16 November 2021, the Group Senior Manager, Financial Crime Investigations & Screening stated he wanted to finalise senior management approval for Customer 41. No conclusion was reached.

See particulars to paragraph 1649.

1653. On 26 March 2021, Crown Melbourne rated Customer 41 high risk.

Particulars

Crown Melbourne rated Customer 41's risk to be high on 26 March 2021: see paragraph 1642.

1654. When Crown Melbourne rated Customer 41 high risk, Crown Melbourne was required to apply its ECDD program to Customer 41.

Particulars

Rule 15.9(1) of the Rules.

See paragraph 661.

1655. Crown Melbourne did not carry out appropriate risk-based ECDD measures with respect to Customer 41 when it rated Customer 41 high risk.

Particulars

See paragraph 1652.

1656. By reason of the matters pleaded from paragraphs 1638 to 1655, on and from 1 March 2016, Crown Melbourne:

a. did not monitor Customer 41 in relation to the provision of designated services, with a view to identifying, mitigating and managing the ML/TF risks reasonably faced; and

b. did not do so in accordance with rr 15.5 and 15.9 of the Rules.

1657. By reason of the matters pleaded at paragraph 1656, Crown Melbourne contravened s36(1) of the Act on and from 1 March 2016 with respect to Customer 41.

Particulars

Section 36(1) of the Act is a civil penalty provision: s36(2) of the Act.

Customer 42

1658. Customer 42 has been a customer of Crown Perth since 1 May 2014.

1659. From at least 1 May 2014, Crown Perth provided Customer 42 with designated services within the meaning of table 1 and table 3, s6 of the Act.

1660. From at least 1 May 2014, Customer 42 received designated services as a junket player facilitated through his own junket, and junket operator at Crown Perth.

Particulars to paragraphs 1659 and 1660

On 1 January 2014, Crown Perth entered into a NONEGPRA with Customer 42 to operate junkets at Crown Perth. Between 2014 and 2016, Customer 42 facilitated at least six junket programs at Crown Perth.

Customer 42 received designated services as a junket player under his own junket programs.

On 1 May 2014, Crown Perth opened a DAB account and a safekeeping account for Customer 42 under two PIDs.

On 28 April 2014, Crown Perth approved a credit facility (AUD/HKD) for Customer 42 under two PIDs. On 15 January 2018, Crown Perth closed this credit facility.

The ML/TF risks posed by Customer 42

1661. By 1 March 2016, higher ML/TF risks were indicated by the nature and purpose of Customer 42's business relationship with Crown Perth, the nature of the transactions he had been conducting, together with the suspicions Crown Perth itself had formed with respect to Customer 42.

Particulars

Section 36(1)(a), (b) of the Act and Chapter 15 of the Rules.

Customer 42 was a junket player and junket operator. He received designated services through the channel of junket programs. This channel lacked transparency: see paragraph 477.

Customer 42 ran at least five junket programs at Crown Perth in 2014 and 2015. Crown Perth recorded that the turnover for these programs was at least $263,893,951. Commissions of 1,847,259 were payable by Crown Perth to Customer 42.

SMRs

By 1 March 2016, Crown Perth had given the AUSTRAC CEO three SMRs in relation to Customer 42 on 9 May 2014, 13 May 2014 and 28 May 2015, which reported as follows:

- on 4 May 2014, Crown Perth sent $680,000, by telegraphic transfer, to a third party company in Australia, at Customer 42's request. Customer 42 had advised Crown Perth that this company was his business partner;
- on 7 May 2014, Crown Perth sent a further $48,000, by telegraphic transfer, to the same third party company in Australia at Customer 42's request. Crown Perth had formed suspicions regarding the authenticity of the relationship between Customer 42 and the third party company; and
- on 28 May 2015, Crown Perth sent $277,634 by telegraphic transfer to Crown Melbourne, for the benefit of one of Customer 42's key players on junket programs at Crown

Melbourne. Customer 42 advised Crown Perth that this was to settle the key player's program, however it was inconsistent with the key player's noted winnings of $130,350.

Other red flags

On 31 December 2015, a deposit of $350,000 was made into a Riverbank account from a third party for the benefit of Customer 42, with a transaction narrative that referred to "COMPANY FUNDS PURPOSE".

At no time before 1 March 2016 did Crown Perth take any due diligence steps taken with respect to Customer 42.

1662. On and from May 2018, Customer 42 should have been recognised by Crown Perth as a high risk customer by reason of the matters pleaded at paragraphs 1661, 1664, 1665 and 1666.

Particulars

Section 36(1)(a), (b) of the Act and Chapter 15 of the Rules.

1663. At no time was Customer 42 rated high risk by Crown Perth.

Particulars

On various occasions between 5 January 2014 and 18 May 2015, Crown Melbourne assessed Customer 42 as low risk.

See paragraph 481.

1664. On and from 1 March 2016, designated services provided to Customer 42 posed higher ML/TF risks including because the provision of designated services to Customer 42 involved a combination of the following factors:

a. Customer 42 received high value financial (table 1, s6) and gaming services (table 3, s6) provided through junket programs: see paragraph 473ff;

b. Customer 42 was a junket operator who facilitated the provision of high value financial and gaming services (tables 1 and 3, s6) to key players (including foreign PEPs) on his junket programs: see paragraph 473ff;

c. Customer 42 was a junket operator and junket player;

d. designated services provided to Customer 42 lacked transparency as the services were provided through the channel of junket programs: see paragraph 477(e);

e. the table 3, s6, designated services provided to Customer 42 involved high turnover and high losses;

f. designated services provided to Customer 42 involved large transfers to and from third parties, including to and from foreign remittance service providers and unknown third party companies: see paragraph 456ff;

g. designated services provided to Customer 42 involved large cross-border movements of funds, including through the Riverbank accounts: see paragraph 239;

h. large values were transferred to and from Customer 42's bank accounts and his DAB account, and to and from other customers' DAB accounts, involving the provision by

Crown Melbourne of designated services within the meaning of items 31 and 32, table 1, s6 of the Act: see paragraphs 411ff and 492;

i. at various times, Customer 42 was provided with significant amounts of credit upon request, up to limits of $6,500,000: see paragraphs 280ff and 487;

j. in May 2016, Crown Melbourne made the Crown private jet available for Customer 42. There were inadequate controls on the carrying of large amounts of cash on Crown's private jets: see paragraphs 454 and 491(c);

k. in 2016, Customer 42 incurred a large debt to Crown, which was repaid through foreign remittance service providers in 2018;

l. these transactions took place against the background of:

   i. Crown Perth giving the AUSTRAC CEO three SMRs relating to Customer 42 by 1 March 2016;

   ii. Customer 42's junkets turning over $263,893,951 in 2014 and 2015;

   iii. Customer 42 receiving a number of suspicious third party transfers; and

   iv. a deposit of $350,000 was made into a Riverbank account from a third party for the benefit of Customer 42 with a narrative that was inconsistent with the funds being used for gaming purposes; and

m. by reason of the matters set out at subparagraphs a. to l. above, there were higher ML/TF risks associated with Customer 42's source of wealth/funds.

Monitoring of Customer 42's transactions

1665. At no time did Crown Perth appropriately monitor Customer 42's transactions on a risk-basis.

Particulars

Section 36(1)(a), (b) of the Act and Rules 15.4 to 15.8 of the Rules.

Crown Perth was unable to monitor the ML/TF risks posed by Customer 42's transactions appropriately because it did not make and keep appropriate records of designated services provided to junket players or operators: see paragraph 483ff.

Crown Perth did not apply appropriate risk-based transaction monitoring to designated services provided to Customer 42: see paragraphs 590ff and 629 to 642 and 643 to 649.

2021 transaction review

In 2020, an independent expert identified that a third party foreign remittance service provider had deposited $539,953 on 14 March 2016 into a Riverbank account for the benefit of Customer 42.

Inadequate cash controls on Crown's private jets

On 19 May 2016, Crown Melbourne provided Customer 42 with access to a Crown private jet from Melbourne to a foreign country for 7 people.

There were inadequate controls on the carrying of large amounts of cash on Crown's private jets: see paragraphs 454 and 491(c).

Ongoing customer due diligence

1666. On and from May 2018, the provision of designated services to Customer 42 by Crown Perth raised red flags reflective of higher ML/TF risks arising from:

a. Customer 42's junket activity; and

b. Customer 42's use of foreign remittance service providers to repay a debt owed to Crown Perth.

Particulars

See paragraph 420ff and 477.

Large and unusual transactions and patterns of transactions in 2016

See the particulars to paragraph 1665.

Between 20 May 2016 and 22 May 2016, Customer 42 operated a junket program and played on a junket program at Crown Perth. Turnover for the programs were $67,142,829 and $10,398,571. Crown management approved a credit facility for use by Customer 42 for the junket program, up to limits of $6,500,000.

Following the close of the junket program, Customer 42 owed a debt to Crown Perth of $6,425,562.

Large and unusual transactions and patterns of transactions in 2018

From approximately May 2018, multiple large payments were made by a foreign remittance service provider to Crown Perth for the benefit of Customer 42, and were used to repay Customer 42's debt, as follows:

A third party, Person 48, an employee of Person 56, a foreign remittance service provider, sent the following to Crown Perth for the benefit of Customer 42:

- on 31 May 2018, a telegraphic transfer of AU$254,598 in a foreign currency;
- on 6 June 2018, a telegraphic transfer of AU$250,246 in a foreign currency; and
- on 6 July 2018, two telegraphic transfers in the amount of AU$259,355 each in a foreign currency.

On 11 July 2018, a different third party, Person 32, also identified as an employee of Person 56, sent a telegraphic transfer in the amount of $856,898 to Crown Perth for the benefit of Customer 42.

The funds received were used by Crown Perth to repay Customer 42's debt.

See paragraphs 332ff and 359ff.

1667. On and from May 2018, Crown Perth failed undertake appropriate risk-based customer due diligence with respect to Customer 42 with a view to identifying, mitigating and managing the ML/TF risks posed by the provision of designated services on and from 1 March 2016.

a. At no time did Crown Perth take appropriate steps to understand whether Customer 42's source of wealth/funds was legitimate.

b. At no time did Crown Perth take appropriate steps to identify or analyse the ML/TF risks of Customer 42's transactions or to consider whether they had a lawful purpose.

c. At no time did Crown Perth give appropriate consideration to whether large and high risk transactions should be processed.

d. At no time did senior management consider whether continuing the business relationship with Customer 42 was within Crown Perth's ML/TF risk appetite.

Particulars

Section 36(1)(a) of the Act.

The due diligence steps taken with respect to Customer 42 included:

Wealth reports

On 26 February 2016, the Credit control team obtained a wealth report on Customer 42, which was relied on by Crown Perth.

Database searches

On 9 March 2016, the Credit control team performed company searches, risk intelligence searches and open source searches, which was relied on by Crown Perth. None of these steps were proportionate to the ML/TF risks reasonably posed by Customer 42 on and from May 2018.

1668. By reason of the matters pleaded from paragraphs 1658 to 1667, on and from May 2018, Crown Perth:

a. did not monitor Customer 42 in relation to the provision of designated services, with a view to identifying, mitigating and managing the ML/TF risks reasonably faced; and

b. did not do so in accordance with rr 15.5 and 15.9 of the Rules.

1669. By reason of the matters pleaded at paragraph 1668, Crown Perth contravened s36(1) of the Act on and from May 2018 to with respect to Customer 42.

Particulars

Section 36(1) of the Act is a civil penalty provision: s36(2) of the Act.

Customer 43

1670. Customer 43 was a customer of Crown Melbourne from 12 April 2012 to 4 February 2020.

1671. From at least 12 April 2012 to 4 February 2020, Crown Melbourne provided Customer 43 with designated services within the meaning of table 1 and table 3, s6 of the Act.

Particulars

On 15 March 2015, Crown Melbourne opened a DAB account and a safekeeping account (AUD) for Customer 43, which were closed on 11 November 2021.

On 5 June 2019, Crown Melbourne opened a second DAB account and safekeeping account (AUD) for Customer 43, which were closed on 11 November 2021.

On 4 February 2020, Crown Melbourne issued a WOL in respect of Customer 43.

Between 2012 and 2015, Crown Melbourne recorded Customer 43's individual rated gaming activity to be a cumulative buy-in of $100,600 with a cumulative loss of $98,150.

Between 2018 and February 2020, Crown Melbourne recorded Customer 43's individual rated gaming activity to be a cumulative buy-in of $5,465,055 with a cumulative loss of $3,722,919.

Customer 43's individual rated gaming activity at Crown Melbourne to February 2020 was a cumulative loss of $3,821,069.

As at 19 January 2022, Customer 43's had a DAB account had a balance of $9,931. The balance of Customer 43's DAB account has not changed since 1 August 2020.

1672. From at least 2012 to February 2020, Customer 43 received designated services as a junket player at Crown Melbourne, facilitated through five different junket operators.

Particulars

Customer 43 received designated services through the Customer 5 and Customer 15 junkets as well as three other junkets.

Customer 43 was a junket representative for the Customer 5 junket and another junket.

Between 2012 and 2019, Customer 43 attended 13 junket programs at Crown Melbourne. In that period, Customer 43 received a total commission of $2,410,054 (0.80%). Customer 43's junket losses at Crown Melbourne to February 2020 was cumulative loss of $4,443,110 and a cumulative turnover of $301,256,702.

1673. Customer 43 was a customer of Crown Perth from 21 July 2014 to 31 January 2020.

1674. From at least 21 July 2014 to 31 January 2020, Crown Perth provided Customer 43 with designated services within the meaning of table 1 and table 3, s6 of the Act.

1675. From at least 2016 to February 2019, Customer 43 received designated services as a junket player at Crown Perth, facilitated through two different junket operators.

Particulars to paragraphs 1674 and 1675

On 21 July 2014, Crown Perth opened a DAB account and safekeeping account (AUD) for Customer 43, which remains open.

Between 2014 and 2020, Customer 43's individual rated gaming activity recorded losses of over $2,000,000.

On 31 January 2020, Crown Perth issued an NRL in respect of Customer 43.

Customer 43 received designated services through the Person 1 and another junket.

Customer 43 was a junket representative for the Customer 5 and another junket.

Between 2016 and February 2019, Crown Perth recorded Customer 43's individual gaming activity and gaming activity on junket programs as a cumulative turnover of $29,376,898 with a loss of $11,859,584.

The ML/TF risks posed by Customer 43

1676. By 1 March 2016, higher ML/TF risks were indicated by the nature and purpose of Customer 43 business relationship with Crown Melbourne and Crown Perth, the nature of the transactions he had been conducting, together with the suspicions Crown Melbourne and Crown Perth themselves had formed with respect to Customer 43.

Particulars

Section 36(1)(a), (b) of the Act and Chapter 15 of the Rules.

Customer 43 was a junket player. He received designated services through the channel of junket programs. This channel lacked transparency: see paragraph 477.

SMRs by 1 March 2016

On 20 March 2015, Crown Melbourne had given the AUSTRAC CEO one SMR in relation to Customer 43. The SMR described Customer 43's rated gaming activity.

On 25 July 2014, Crown Perth had given the AUSTRAC CEO one SMR in relation to Customer 43. The SMR described that Customer 43 had withdrawn $71,841 which had been transferred from another Crown Perth patron and did not correspond to his recorded program play. Crown Perth understood the customers to be business partners. A risk intelligence search returned that Customer 43 was a foreign PEP.

Gaming activity by 1 March 2016

Between 2012 and 2015, Crown Melbourne recorded Customer 43's individual rated gaming activity to be a cumulative buy-in of $100,600 with a cumulative loss of $98,150.

Due diligence conducted by 1 March 2016

On 24 July 2014, Crown Perth first determined Customer 43 to be a foreign PEP.

On 8 August 2014, a Crown Perth Legal Officer (AML) conducted ECDD in respect of Customer 43 and approved a continuing business relationship with Customer 43 despite his status as a foreign PEP.

On 21 August 2014, a Crown Vice President in the international business team identified Customer 43 to be a foreign PEP, that Customer 43 was attending Crown Perth for the first time and that he was not playing on a program but instead was playing with cash chips. Crown Perth rated Customer 43's risk as high.

On 20 March 2015, Crown Melbourne first determined Customer 43 to be a foreign PEP as a result of a risk intelligence search which returned a match. Crown Melbourne rated Customer 43's risk as high. An Executive General Manager (Legal & Regulatory Services) approved Crown Melbourne continuing a business relationship with Customer 43 despite being a foreign PEP.

1677. At all times on and from 1 March 2016, Customer 43 was rated as high risk by Crown Melbourne and Crown Perth.

Particulars

On various occasions after 8 August 2014, Crown Perth rated Customer 43's risk as high.

On various occasions after 20 March 2015, Crown Melbourne rated Customer 43's risk as high.

See paragraph 481.

1678. On and from 1 March 2016 designated services provided to Customer 43 posed higher ML/TF risks, including because the provision of designated services to Customer 43 involved a combination of the following factors:

a. Customer 43 was a foreign PEP: see paragraphs 118 and 663;

b. Customer 43 was a junket player and junket representative;

c. Customer 43 received large value financial (table 1, s6) and gaming services (table 3, s6) provided through multiple junket programs: see paragraph 473ff;

d. by February 2019, Crown Perth recorded Customer 43's individual gaming activity and gaming activity on junket programs as a cumulative turnover of $29,376,898 with a loss of $11,859,584;

e. by February 2020, Crown Melbourne recorded Customer 43's cumulative turnover of $301,256,702 with a cumulative loss of $4,443,110;

f. designated services provided to Customer 43 involved a lack of transparency as the services were provided through the channel of junket programs: see paragraph 477(e);

g. Customer 43 regularly made transfers to or received transfers from third parties and junket operators including Customer 5 and foreign remittance service providers, including Person 56: see paragraph 332ff, 359ff and 456ff;

h. designated services provided to Customer 43 involved large cross-border movements of funds including from money changers: see paragraph 239;

i. Crown Melbourne senior management approved an early release of funds for Customer 43, being a loan for the purpose of item 6, table 1 s6 services, on a number of occasions: see paragraph 395ff;

j. at various times, Customer 43 had significant parked or dormant funds in his DAB accounts: see paragraph 252;

k. Customer 43 carried and transacted in large cash values and regularly would deposit large amounts of cash in a foreign currency and withdraw it in Australian dollars;

l. Crown Melbourne transferred large values of funds to and from Customer 43's bank accounts and his DAB account (items 31 and 32, table 1, s6 of the Act);

m. by November 2018, Crown was aware that Customer 43 was implicated in a graft case involving the reported misuse of public funds. By January 2019, Crown was aware that Customer 43 had been called on by a corruption commission. By November 2019, Crown was aware that Customer 43 had been charged by election authorities with voter intimidation;

n. in January 2019, Customer 43 made seven cash deposits at Crown Perth indicative of the ML/TF typology of structuring;

o. in November 2016 and January 2017, Customer 43 received three telegraphic transfers into his Crown Perth DAB account indicative of the ML/TF typology of cuckoo smurfing; and

p. by reason of the matters set out at subparagraphs a. to o. above, there were real risks that Customer 43's source of wealth and source of funds were not legitimate.

Monitoring of Customer 43's transactions

1679. At no time did Crown Melbourne or Crown Perth appropriately monitor Customer 43's transactions on a risk-basis.

Particulars

Section 36(1)(a), (b) of the Act and Rules 15.4 to 15.8 of the Rules.

Crown Melbourne and Crown Perth were unable to monitor the ML/TF risks posed by Customer 43's transactions appropriately because they did not make and keep appropriate records of designated services provided to junket players: see paragraph 483ff.

Crown Melbourne and Crown Perth did not apply appropriate risk-based transaction monitoring to designated services provided to Customer 43: see paragraphs 590ff and 629 to 642.

Customer 43's transactions involved repeated transactions indicative of ML/TF typologies and vulnerabilities that were not detected prior to a 2020 and 2021 lookback. Had appropriate risk-based transaction

monitoring been applied, these transactions could have been identified earlier: see paragraphs 686 and 687.

In 2020 and 2021, independent auditors identified the following transactions of Customer 43 as indicative of ML/TF typologies:

- on 21 November 2016, Customer 43 received $96,199 from Person 10. This was indicative of the ML/TF typology of cuckoo smurfing; and
- between 4 January 2019 and 8 January 2019, Customer 43 made seven cash deposits at Crown Perth ranging from $300 to $6,500 totalling $24,800. This transaction was indicative of the ML/TF typology of structuring.

Transactions with third party remitter (Person 56)

On and from 21 September 2016, Customer 43 was involved in a number of complex, unusual large transactions and unusual patterns of transactions from a third party remitter, Person 56, and owner of a money changer in South East Asia, Company 10: see paragraph 332ff and 359ff. These transactions had no apparent economic or visible lawful purpose:

- on 21 September 2016, the third party remitter (Person 56) deposited $100,050 by telegraphic transfer into her own Crown Perth DAB account. On 22 September 2016, Person 56 provided an authority to disperse form requesting that the amount be transferred to another Crown Perth customer who was Customer 43's assistant. That customer then withdrew $90,000 from his DAB account and transferred it to Customer 43's DAB account. Crown Perth was not aware of any reason for the transaction: SMR dated 28 September 2016;
- on 17 November 2016, Customer 43 received at Crown Perth $194,968 from the third party remitter, Person 56. In 2020, an independent auditor found this transaction to be indicative of the ML/TF typology of transactions involving third parties;
- on 17 November 2016, an Executive General Manager (Legal and Corporate Services) approved the early release of $195,000 from Customer 43 held by the third party remitter (Person 56) through her money changer, Company 10, which was to be remitted to a Riverbank account that day. This constituted item 6 table 1 services. The funds were transferred to Customer 43 from Person 56;
- on 9 January 2017, Customer 43 received at Crown Perth a telegraphic transfer of $189,968 from the third party remitter, Person 56. In 2020, an independent auditor found this transaction to be indicative of the ML/TF typology of transactions involving third parties;
- on 8 July 2018 Customer 43 received $100,000 from the money changer run by the third party remitter, Company 10;

- on 8 January 2020, Customer 43 was involved in a $1,500,000 transaction. On 8 January 2020, Crown Melbourne received a letter from the third party remitter, Person 56, at her money changers, Company 10, stating that she had received a large sum in a foreign currency as security to purchase AUD1,500,000 for further credit of Customer 43's Crown Melbourne's account. On 9 January 2020, a Group General Manager (AML) emailed an Employee Licensing Officer and Manager (Program Compliance) asking whether they received the transaction and stating that he needed to explain how Crown reported such transactions. Senior management approved the early release of funds. This constituted item 6 table 1 services. As at 13 March 2020, despite the funds having been released early, only $300,000 had been received by Crown; and
- on 13 January 2020, Customer 43 received at Crown Perth a telegraphic transfer of $177,820 from the third party remitter, Person 56.

Ongoing customer due diligence

1680. On and from 1 March 2016, on multiple occasions, the provision of designated services to Customer 43 raised red flags reflective of higher ML/TF risks as a result of complex, unusual large transactions and unusual patterns of transactions involving Customer 43 which had no apparent economic or visible lawful purpose.

Particulars

See paragraphs 435, 450, 451, 477 and 491.

Large unusual transactions and unusual patterns of transactions in 2016

On 18 November 2016, Customer 43 cashed out $80,000 followed by $50,000 worth of chips at Crown Perth. Customer 43 had significant recorded play, but the transactions were noted to be unusual. Crown Perth rated Customer 43's risk as high: SMR dated 22 November 2016.

Large unusual transactions and unusual patterns of transactions in 2018

Between 2015 and July 2018, Customer 43's average bet increased from $3,935 to $6,553. Crown Melbourne rated Customer 43's risk as high: SMR dated 9 July 2018.

On 9 July 2018, Customer 43 purchased a large sum in a foreign currency.

On 26 July 2018, Customer 43 received $252,709 from Crown Perth.

On 27 July 2018, Customer 43 made an account deposit of $106,588 and a cash withdrawal of $20,088.

On 31 July 2018, Customer 43 received $270,000 from a third party.

By 2 August 2018, Customer 43 was a key player on a junket program at Crown Melbourne and recorded a loss of $550,000. Crown Melbourne rated Customer 43's risk as high: SMR dated 2 August 2018.

By 8 August 2018, Customer 43's recorded loss increased to $717,055. Crown Melbourne rated Customer 43's risk as high: SMR dated 8 August 2018.

On 7 August 2018, Customer 43 made a chip cash-in of $11,500.

On 9 August 2018, Customer 43 took two chip redemption gaming cheques for $130,000 and $100,000.

On 10 August 2018, Customer 43 transferred $100,000 to himself.

Between 30 July 2018 and 13 August 2018, Customer 43 was a key player on a junket program at Crown Melbourne.

Between 2015 and 2018, Customer 43's Crown Melbourne individual loss had increased from $97,740 with a buy-in of $100,000, to $759,112 with a buy-in of $1,308,000.

Between 2012 and 2018, Customer 43's Crown Melbourne junket turnover had increased significantly from $159,200 to $85,253,690.

Large unusual transactions and unusual patterns of transactions in 2019

On 2 January 2019 and 3 January 2019, while a key player on a junket, Customer 43 transferred into his Crown Perth DAB account three large sums in foreign currency. After each deposit, Customer 43 withdrew the majority of the funds as CPVs, which he exchanged for chips and used for gaming activity.

On 8 January 2019, Customer 43 made two chip deposits into his Crown Perth DAB account of $50,000 and $35,000 which he then withdrew in cash. Crown Perth rated Customer 43's risk as high: SMR dated 4 February 2019.

On 16 January 2019, Customer 43 received two machine payouts which totalled $39,796.45.

In January 2019, Customer 43 was a key player in a junket program and recorded a loss of $400,000. Crown Melbourne rated Customer 43's risk as high: SMR dated 16 January 2019.

On 1 March 2019, Customer 43 received a transfer of $200,000 from Customer 5, a junket operator.

By June 2019, Customer 43 had junket losses at Crown Melbourne in 2018 and 2019 of approximately $3,600,000. Crown Melbourne rated Customer 43's risk as high: SMR dated 21 June 2019.

Between 31 May 2019 and 30 June 2019, Customer 43 was a key player in a Customer 5 junket program.

On 1 August 2019, Crown Perth last provided a designated service to Customer 43.

Between 2018 and 2019, Customer 43's Crown Melbourne junket turnover had increased significantly from $85,253,690 to $201,107,490. His corresponding junket loss, from $1,540,480 to $2,126,530, did not increase significantly.

Large unusual transactions and unusual patterns of transactions in 2020

In January 2020, Customer 43 had losses under the Customer 5 junket and another junket of approximately $1,000,000 together with individual losses of over $2,000,000 over the same period.

On 31 January 2020, Crown Perth issued an NRL in respect of Customer 43.

On 4 February 2020, Crown Melbourne issued a WOL in respect of Customer 43 as a result of the SPR process.

1681. At no time did Crown Melbourne or Crown Perth undertake appropriate risk-based customer due diligence with respect to Customer 43 with a view to identifying, mitigating and managing the ML/TF risks posed by the provision of designated services on and from 1 March 2016.

a. At no time did Crown Melbourne or Crown Perth take appropriate steps to understand whether Customer 43's source of wealth/funds was legitimate.

b. At no time did Crown Melbourne or Crown Perth take appropriate steps to identify or analyse the ML/TF risks of Customer 43's transactions or to consider whether they had a lawful purpose.

c. At no time did Crown Melbourne or Crown Perth give appropriate consideration to whether large and high risk transactions should be processed.

d. On each occasion prior to February 2020 that senior management considered whether to continue the business relationship with Customer 43, senior management failed to give adequate consideration to whether the ML/TF risks posed by Customer 43 were within Crown Melbourne and Crown Perth's risk appetite.

Particulars

Section 36(1)(a) of the Act.

The due diligence steps taken with respect to Customer 43 included:

Player reviews

On 16 January 2019, Crown Melbourne conducted a key player review in respect of Customer 43 which identified him to be a foreign PEP.

Due diligence searches

In November 2018, July 2019 27 November 2019 and 15 January 2020, Crown conducted risk intelligence searches in respect of Customer 43.

On 15 January 2020, Crown Melbourne conducted a media report search in respect of Customer 43. The search returned articles published between December 2005 and September 2019 concerning Customer 43's public career in a foreign country, including that he had been charged with voter intimidation and had refused to comply with police summons for questioning as a witness in a graft case.

By 24 January 2020, Crown Melbourne was aware that Customer 43's monthly salary and net worth were not commensurate with his gaming activity. Crown Melbourne were aware that Customer 43 had been reported to the relevant Ministry for numerous travels abroad not related to his duties and under suspicion that Customer 43 was travelling abroad to launder money in casinos for high sums in a foreign currency: SMR dated 24 January 2020.

Wealth reports

In July 2019, Crown Melbourne prepared a credit profile for Customer 43 for the purpose of assessing his creditworthiness.

In November 2019, Crown Melbourne obtained a wealth report in respect of Customer 43 for the purpose of assessing his creditworthiness. The report included that Customer 43 was in a high wealth band. The report stated that Customer 43 was a foreign PEP.

Senior management engagement

On 27 September 2016, a Vice President (International Guest Services) identified Customer 43 to be a foreign PEP and another Crown patron as Customer 43's assistant.

In January 2019, Crown Melbourne became aware of media articles published in September 2017 which reported that Customer 43 was called on by a corruption commission in a foreign country as a suspect in a graft case. Customer 43 was later named as a witness in a graft case involving the misappropriation of funds. After Crown Melbourne became aware of the September 2017 media article, the AML Manager (Crown Melbourne) determined to review Customer 43's gaming activities. There is no evidence that she did so.

In February 2019, the CTRM reviewed Customer 43's patron details and risk rating.

None of these steps were proportionate to the ML/TF risks reasonably posed by Customer 43 on and from 1 March 2016.

Customer 43 banned from Crown Melbourne and Crown Perth

On 21 January 2020, the AML Manager (Crown Melbourne) emailed Crown senior management due diligence held by Crown in respect of Customer 43. The email stated that Customer 43 presented a significant reputational risk to Crown from a financial perspective because of Customer 43's position in a foreign country, his monthly salary, his unverified source of wealth in respect of the amount of

gaming losses he had experienced and the numerous media articles which suggested public corruption and the siphoning off of public funds.

The AML Manager (Crown Melbourne) recommended that senior management re-assess the continuing relationship with Customer 43.

A Senior Vice President (International Business) responded that Crown Melbourne should obtain more due diligence to verify his source of funds.

On 3 February 2020, Crown Perth issued an NRL in respect of Customer 43.

In February 2020, Crown Melbourne were aware that Customer 43's net worth in 2018 was not commensurate with his gaming activity: SMR dated 4 February 2020.

The POI Committee made the decision to end Crown's business relationship with Customer 43. Crown Melbourne issued a WOL in respect of Customer 43 on 4 February 2020.

Enhanced customer due diligence

1682. Having formed a suspicion for the purposes of s41 of the Act, Crown Melbourne gave the AUSTRAC CEO SMRs with respect to Customer 43 on:

a. 9 July 2018;

b. 27 July 2018;

c. 2 August 2018;

d. 8 August 2018;

e. 16 January 2019;

f. 21 June 2019;

g. 24 January 2020; and

h. 4 February 2020.

Particulars

The 9 July 2018 to 21 June 2019 SMRs described Customer 43's annual individual and junket losses, increase in average bet and the amount of cash Customer 43 was prepared to carry.

The 24 January 2020 and 4 February 2020 SMRs reported that:

- Customer 43 had been identified to be a foreign PEP with links to alleged corruption;
- Customer 43 had a high net worth according to a wealth report;
- Customer 43 had been reported to a Minister for travel abroad unrelated to his public duties and it was suspected that he did so to launder money in casinos; and

- Customer 43's source of wealth was unverified given the level of losses he accumulated.

1683. On each occasion that Crown Melbourne formed a suspicion with respect to Customer 43 for the purposes of s41 of the Act, it was required to apply its ECDD program to Customer 43.

Particulars

Rule 15.9(3) of the Rules.

1684. Crown Melbourne did not carry out appropriate risk-based ECDD measures with respect to Customer 43 on each occasion that Crown Melbourne formed a suspicion with respect to Customer 43 for the purposes of s41 of the Act.

a. There are no records of ECDD being conducted following the lodgement of SMRs on 9 July 2018, 27 July 2018, 2 August 2018, 8 August 2018, 21 June 2019: see paragraphs 664 and 685.

b. Appropriate risk-based steps were not taken to obtain or analyse information about Customer 43's source of wealth/funds, including the legitimacy of those funds: see paragraph 667. The SMRs given to the AUSTRAC CEO on 24 January 2020 and 4 February 2020 expressly included that Customer 43's source of wealth was unconfirmed and unverified considering the level of losses he had accumulated.

c. Appropriate risk-based steps were not taken to analyse and monitor Customer 43's transactions – both past and future – including to understand their economic purpose: see paragraphs 590 and 666.

d. On each occasion prior to February 2020 that senior management considered whether to continue the business relationship with Customer 43, senior management failed to give adequate consideration to whether the ML/TF risks posed by Customer 43 were within Crown Melbourne's risk appetite.

Particulars

Rules 15.9(3), 15.10(1)(c), (d), (2), (5) and (6) of the Rules.

See particulars to paragraph 1681.

1685. Having formed a suspicion for the purposes of s41 of the Act, Crown Perth gave the AUSTRAC CEO SMRs with respect to Customer 43 on:

a. 28 September 2016;

b. 22 November 2016; and

c. 4 February 2019.

Particulars

The SMRs reported suspicions arising in relation to transactions involving two Crown Perth customers and Customer 43: see paragraph 1679.

1686. On each occasion that Crown Perth formed a suspicion with respect to Customer 43 for the purposes of s41 of the Act, it was required to apply its ECDD program to Customer 43.

Particulars

Rule 15.9(3) of the Rules.

1687. Crown Perth did not carry out appropriate risk-based ECDD measures with respect to Customer 43 on each occasion that Crown Perth formed a suspicion with respect to Customer 43 for the purposes of s41 of the Act.

a. There are no records of ECDD being conducted following the lodgement of SMRs on 28 September 2016, 22 November 2016 and 4 February 2019: see paragraphs 664 and 685.

b. Appropriate risk-based steps were not taken to obtain or analyse information about Customer 43's source of wealth/funds: see paragraph 667.

c. Appropriate risk-based steps were not taken to analyse and monitor Customer 43's transactions – both past and future – including to understand their economic purpose: see paragraphs 590 and 666.

d. The only ECDD recorded by Crown Perth as being conducted in respect of Customer 43 was in August 2014 and February 2020.

e. On each occasion prior to February 2020 that senior management considered whether to continue the business relationship with Customer 43, senior management failed to give adequate consideration to whether the ML/TF risks posed by Customer 43 were within Crown Perth's risk appetite: see paragraph 668ff.

Particulars

Rules 15.9(3), 15.10(1)(c), (d), (2), (5) and (6) of the Rules.

See particulars to paragraph 1681.

1688. At all times from 1 March 2016, Customer 43 was a foreign PEP.

Particulars

Section 36(1)(a) of the Act.

Customer 43 had been identified to be a foreign PEP with links to alleged corruption.

1689. At all times from 1 March 2016, Crown Melbourne and Crown Perth were required to apply its ECDD program to Customer 43.

Particulars

Rules 15.9(2) and 15.11 of the Rules.

See paragraphs 660, 663 and 666.

1690. Crown Melbourne and Crown Perth did not carry out appropriate risk-based ECDD measures with respect to Customer 43 on and from 1 March 2016 given his status as a foreign PEP. In particular:

a. Crown Melbourne did not undertake a detailed analysis of Customer 43's KYC information or analyse the legitimacy of Customer 43's source of wealth/funds;

b. prior to the decision to issue Customer 43 with a WOL and NRL in early 2020, there is no record of senior management approval for continuing a business relationship with Customer 43 as a foreign PEP having have adequate regard to the ML/TF risks posed by Customer 43 given his status as a foreign PEP on and from 1 March 2016; and

c. prior to the decision to issue Customer 43 with a WOL and NRL in early 2020, there is no record of senior management approval for continuing to provide designated services to Customer 43 as a foreign PEP having adequate regard to the ML/TF risks posed by Customer 43 given his status as a foreign PEP on and from 1 March 2016.

Particulars

Rules 15.10(2), 15.10(6), 15.11 of the Rules.

See paragraphs 1681, 1684 and 1687.

See paragraph 660, 663, 666, 667 and 668.

1691. On and from 1 March 2016, Crown Melbourne and Crown Perth rated Customer 43 high risk.

Particulars

Crown Melbourne rated Customer 43 high risk on seven occasions on and from 20 March 2015: paragraph 1677.

Crown Perth rated Customer 43 high risk on 19 occasions on and from 8 August 2014: paragraph 1677.

1692. On each occasion that Crown Melbourne and Crown Perth rated Customer 43 high risk, Crown Melbourne and Crown Perth was required to apply its ECDD program to Customer 43.

Particulars

Rule 15.9(1) of the Rules.

See paragraph 661.

1693. Crown Melbourne and Crown Perth did not carry out appropriate risk-based ECDD measures with respect to Customer 43 on each occasion that Crown Melbourne and Crown Perth rated Customer 43 high risk.

Particulars

See paragraphs 1681, 1684, 1687 and 1690.

See paragraphs 661, 666, 667 and 668.

1694. By reason of the matters pleaded from paragraphs 1670 to 1693, on and from 1 March 2016, Crown Melbourne and Crown Perth:

a. did not monitor Customer 43 in relation to the provision of designated services, with a view to identifying, mitigating and managing the ML/TF risks reasonably faced; and

b. did not do so in accordance with rr 15.5 and 15.9 of the Rules.

1695. By reason of the matters pleaded at paragraph 1694, Crown Melbourne contravened s36(1) of the Act on and from 1 March 2016 to February 2020 with respect to Customer 43.

Particulars

Section 36(1) of the Act is a civil penalty provision: s36(2) of the Act.

1696. By reason of the matters pleaded at paragraph 1694, Crown Perth contravened s36(1) of the Act on and from 1 March 2016 to 31 January 2020 with respect to Customer 43.

Particulars

Section 36(1) of the Act is a civil penalty provision: s36(2) of the Act.

Customer 44

1697. Customer 44 has been a customer of Crown Melbourne since 14 July 2000.

1698. From at least December 2006, Crown Melbourne provided Customer 44 with designated services within the meaning of table 1 and table 3, s6 of the Act.

Particulars

On 15 February 2002, Crown Melbourne opened a DAB account and a safekeeping account (AUD) for Customer 44 which remains open.

Between 2000 and 2015, Crown Melbourne recorded Customer 44's individual gaming activity to be a cumulative buy-in of $4,796,301 with a loss of $386,908.

Between 2016 and 2019, Crown Melbourne recorded Customer 44's individual gaming activity to be a cumulative buy-in of $9,160,000 with a loss of $362,110.

1699. From at least 1 December 2017, Customer 44 received designated services as a junket player, facilitated through the Suncity junket.

Particulars

Customer 44 received designated services through the Suncity junket.

Between 1 December 2017 and 31 August 2019, Customer 44 was a key player in 16 junket programs operated by Suncity at Crown Melbourne with a cumulative turnover of $49,050,000 and HKD37,360,000, a cumulative loss of $177,670 and a cumulative win of HKD6,174,250.

1700. Customer 44 has been a customer of Crown Perth since 7 May 2004.

1701. From at least 4 March 2016, Crown Perth provided Customer 44 with designated services within the meaning of table 1 and table 3, s6 of the Act.

Particulars

On 7 May 2004, Crown Perth opened a DAB account and a safekeeping account (AUD) for Customer 44 which remains open.

On 2 April 2016, Crown Perth opened a second DAB account and safekeeping account (AUD) for Customer 44 which remains open.

On 4 March 2016, Crown Perth last provided a designated service to Customer 44.

By 9 February 2017, Customer 44 had a turnover at Crown Perth of $300,000 with net Crown win of $0.

The ML/TF risks posed by Customer 44

1702. By 1 March 2016, higher ML/TF risks were indicated by the nature and purpose of the Customer 44's relationship with Crown Melbourne, the nature of the transactions he had been conducting, together with the suspicions Crown Melbourne itself had formed with respect to Customer 44.

Particulars

Section 36(1)(a), (b) of the Act and Chapter 15 of the Rules.

Customer 44 was a junket player. He received designated services through the Suncity junket channel: see paragraph 521ff.

SMRs by 1 March 2016

By 1 March 2016, Crown Melbourne had given the AUSTRAC CEO seven SMRs in relation to Customer 44 – on 1 September 2004, 3 October 2006, 27 August 2008, 30 October 2013, 13 February 2014, 8 August 2014 and 10 February 2015. Each SMR reported the same repeated patterns of suspicions relating to annual win and losses, third party transactions and the amount of cash Customer 44 was prepared to carry.

Collectively, the SMRs given to the AUSTRAC CEO between 1 September 2004 and 8 August 2014 reported total wins of $505,878 and wins losses of $73,400 over this 10 year period.

Large and unusual transactions to 1 March 2016

On 12 February 2014, Customer 44 transferred $126,706 to a third party and $100,000 to a second third party.

On 7 August 2014, Customer 44 received $20,000 from an overseas third party.

On 9 February 2015, Customer 44 sent two telegraphic transfers of $100,000 each from his personal account to his Crown Melbourne DAB account.

Due diligence by 1 March 2016

On 31 March 2015, the Executive General Manager (Legal & Regulatory Services) approved continuing a business relationship with a number of listed PEPs, including Customer 44.

On various occasions between 26 November 2014 and 3 February 2016, Crown Melbourne conducted a risk intelligence search in respect of Customer 44 which determined him to be likely a foreign PEP.

1703. As at 1 March 2016, Customer 44 should have been recognised by Crown Melbourne as a high risk customer for the reasons pleaded at paragraph 1702.

1704. At all times on and from 1 March 2016, Customer 44 should have been recognised by Crown Melbourne as a high risk customer by reason of the matters pleaded at paragraphs 1702, 1706, 1707, 1708, 1710 and 1713.

Particulars

Section 36(1)(a), (b) of the Act and Chapter 15 of the Rules.

1705. From 26 November 2014 to 6 March 2019, Customer 44 was rated high risk by Crown Melbourne. However, at no time after 6 March 2019 was Customer 44 rated high risk by Crown Melbourne despite the matters pleaded at paragraphs 1702, 1706, 1707, 1708, 1710 and 1713.

Particulars

On 26 November 2014, Crown Melbourne determined that Customer 44 was likely to be a foreign PEP. On various occasions between 26 November 2014 and 6 March 2019, Crown Melbourne rated Customer 44's risk as high.

However, on five occasions between 7 March 2019 and 16 February 2021, Crown Melbourne rated Customer 44's risk as moderate. This was despite Customer 44 being a foreign PEP with significant individual and junket turnover.

See paragraph 481.

1706. On and from 1 March 2016 designated services provided to Customer 44 posed higher ML/TF risks including because the provision of designated services to Customer 44 involved a combination of the following factors:

a. Customer 44 was a foreign PEP: see paragraphs 118 and 663;

b. Customer 44 was a junket player;

c. Customer 44 received large value financial (table 1, s6) and gaming services (table 3, s6) provided through a number of Suncity junket programs: see paragraph 473ff;

d. by August 2019, Crown Melbourne recorded Customer 44's junket activity to exceed a cumulative turnover of $49,000,000 and HKD37,000,000, with a cumulative loss of $177,670 and a cumulative win of HKD6,174,250;

e. designated services provided to Customer 44 lacked transparency as the services were provided through the channel of junket programs: see paragraph 477(e);

f. the table 3, s6, designated services provided to Customer 44 involved high turnover;

g. designated services provided to Customer 44 involved large transfers to third parties, including to junket operators;

h. designated services provided to Customer 44 involved large cross-border movements of funds: see paragraph 239;

i. in January 2018, Crown were aware that an unknown person had deposited $980,000 in cash at the Suncity cash administration desk on behalf of Customer 44 and another patron: see paragraph 529 to 531;

j. in February 2020, Crown Melbourne reported to the AUSTRAC CEO that it had been unable to verify Customer 44's source of wealth; and

k. by reason of the matters set out at subparagraphs a. to j. above, there were higher ML/TF risks associated with Customer 44's source of wealth/funds.

Monitoring of Customer 44's transactions

1707. At no time did Crown Melbourne appropriately monitor Customer 44's transactions on a risk-basis.

Particulars

Section 36(1)(a), (b) of the Act and Rules 15.4 to 15.8 of the Rules.

Crown Melbourne was unable to monitor the ML/TF risks posed by Customer 44's transactions appropriately because it did not make and keep appropriate records of designated services provided to junket players: see paragraph 483ff.

Crown Melbourne did not apply appropriate risk-based transaction monitoring to designated services provided to Customer 44: see paragraphs 590ff, 629 to 632 and 643 to 649.

Between 8 July 2018 and 6 June 2019, Customer 44 was involved in high-value transactions with third parties and junket operators:

- on 8 July 2018, Customer 44 received $134,643 (GBP76,005.70) from Crown Aspinalls into his Crown Melbourne DAB account;
- on 29 August 2018 and 22 March 2019, Customer 44 transferred $769,453 (GBP437,896) and $128,715.20 (GBP69,674) respectively from his Crown Melbourne DAB account to Crown Aspinalls;
- between 19 July 2018 and 4 September 2019 Customer 44 received $2,816,425 across seven transactions from Customer 1 into his personal account;
- between 25 August 2018 and 4 September 2018, Customer 44 transferred $455,000 to Customer 1's Crown Melbourne DAB account across six transactions;
- on 28 and 29 January 2019, Customer 44 transferred $150,000 and $300,000 respectively from his Crown Melbourne DAB account to another Crown patron's personal account;
- between 31 March 2016 and 22 August 2018, Customer 44 appears to have transferred approximately $5,100,000 through a Southbank account. The majority of the transactions were Customer 44 funding himself;
- on 14 March 2019, Customer 44 transferred $1,000,000 from his personal account to his Crown Melbourne DAB account; and
- on 23 March 2019, Customer 44 transferred $871,284.80 from his Crown Melbourne DAB account to his personal account.

Ongoing customer due diligence

1708. On and from 1 March 2016, on multiple occasions, the provision of designated services to Customer 44 raised red flags reflective of higher ML/TF risks.

Particulars

See paragraphs 450, 451, 447 and 491.

During the following times, designated services provided to Customer 44 involved complex, unusual large transactions and unusual patterns of transactions which had no apparent economic or visible lawful purpose:

Between 1 December 2017 and 31 August 2019, Customer 44 attended 16 Suncity junket programs with a cumulative turnover of $49,050,000 and HKD37,360,000 with a cumulative loss of $177,670 and a cumulative win of HKD6,174,250.

By 9 February 2017, Customer 44's turnover at Crown Melbourne was $12,000,000 with a net Crown win of $200,000 and his turnover at Crown Perth was $300,000 with a net Crown win of $0.

By 16 March 2017, Customer 44's total turnover had increased to $54,000,000.

Between 24 July 2016 and 13 May 2017, Customer 44 made seven account deposits totalling $222,661, four cash withdrawals totalling $130,337 and two foreign currency buys totalling $51,593 at Crown Melbourne.

On 25 January 2018, an unknown person deposited $980,000 at the Suncity cash administration desk and then left the room without playing and was not issued gaming chips. The identity of the person was understood to be a friend of Customer 44, and the funds were understood to be presented on behalf of Customer 44 and another patron: SMR dated 31 January 2018.

In February 2020, Customer 44 had been a key player under recent junket programs with noted losses of $667,950: SMR dated 24 February 2020.

On 13 February 2020, was involved in a $950,000 transaction on the Crown Melbourne bank account with Customer 1.

On 20 February 2020, Crown Melbourne last provided a designated service to Customer 44.

1709. At no time did Crown Melbourne or Crown Perth undertake appropriate risk-based customer due diligence with respect to Customer 44 with a view to identifying, mitigating and managing the ML/TF risks posed by the provision of designated services on and from 1 March 2016.

a. At no time did Crown Melbourne or Crown Perth take appropriate steps to understand whether Customer 44's source of wealth/funds was legitimate.

b. At no time did Crown Melbourne or Crown Perth take appropriate steps to identify or analyse the ML/TF risks of Customer 44's transactions or to consider whether they had a lawful purpose.

c. At no time did Crown Melbourne or Crown Perth give appropriate consideration to whether large and high risk transactions involving Customer 44 should be processed.

d. On each occasion that senior management considered whether to continue the business relationship with Customer 44, senior management failed to give adequate consideration to whether the ML/TF risks posed by Customer 44 were within Crown Melbourne or Crown Perth's risk appetite.

Particulars

Section 36(1)(a) of the Act.

The due diligence steps taken with respect to Customer 44 included:

Wealth and risk intelligence reports

In December 2016 and August 2018, Crown Melbourne and Crown Perth obtained a risk intelligence report ordered by Crown Aspinalls in respect of Customer 44. The reports included that Customer 44 was a foreign PEP, details on Customer 44's business interests and that Customer 44 had a high net wealth. The August 2018 report identified a media article published in February 2016 which indicated that the acquisition of several companies by Customer 44 and his family had raised suspicion of the possible loss of state assets through fraudulent privatisation.

Crown Melbourne did not take appropriate steps to identify or analyse the ML/TF risks posed by Customer 44.

Database searches

Between January 2017 and December 2020, Crown Melbourne and Crown Perth conducted company searches, land registry searches, bankruptcy searches, open source media searches and risk intelligence searches in respect of Customer 44 and companies associated with Customer 44.

The media searches returned two articles. The first article was published in May 2018 and detailed the upcoming initial public offer of a company associated with Customer 44. The article reported a controversy surrounding the loss of state-owned business assets by Customer 44's purchase of the business. The second article was published in February 2016 and contained no relevant information.

Crown Melbourne did not take appropriate steps to identify or analyse the ML/TF risks posed by Customer 44 following the searches.

Senior management engagement

In February 2017, due diligence was conducted in respect of Customer 44 for the purpose of determining Customer 44's domicile. The due diligence profile included Customer 44's turnover and wins losses, that Customer 44 was a foreign PEP. The recommendation was that Crown Melbourne continue to conduct business with Customer 44.

In March 2017, a VIP Operations meeting took place. The agenda included Customer 44's due diligence profile summary, which noted Customer 44's turnover and last date of visit, being February 2017,

that Customer 44 was a foreign PEP and Customer 44's foreign passport and residential address. The recommendation was that Crown Melbourne allow Customer 44 to visit in future on a cash basis or under a junket program.

In January 2019, an AML Officer sent an email to the CTRM in respect of Customer 44. The AML Officer attached to their email Customer 44's foreign passport, SYCO profile, image and foreign PEP details. Crown Melbourne rated Customer 44's risk as high as a result of this email.

In March 2019, a Credit Analyst (VIP International) sent an email to Crown senior management. The Credit Analyst identified Customer 44 to be an inactive foreign PEP and that he was due at Crown Aspinalls on 9 March 2019. The Credit Analyst attached the February 2019 risk intelligence report. The AML Manager (Crown Melbourne) responded saying that Customer 44 was no longer a PEP because he had not been an active foreign PEP in the previous six months, and so no further action was needed from an AML/CTF perspective. Crown Melbourne decreased Customer 44's risk rating to moderate as a result of this email exchange.

In May 2019, a Group General Manager (VIP International) sent an email to the AML Manager (Crown Melbourne) saying that daily due diligence had revealed that Customer 44, being an inactive foreign PEP, was in-house playing under the Suncity junket program. The Group General Manager attached the May 2019 risk intelligence search. Crown Melbourne rated Customer 44's risk as moderate as a result of the email. Crown Perth rated Customer 44's risk as low as a result of the email and first identified Customer 44 to be a foreign PEP.

None of these steps were proportionate to the ML/TF risks reasonably posed by Customer 44 on and from 1 March 2016.

Enhanced customer due diligence

1710. Having formed a suspicion for the purposes of s41 of the Act, Crown Melbourne gave the AUSTRAC CEO SMRs with respect to Customer 44 on:

a. 24 June 2016;

b. 31 January 2018; and

c. 24 February 2020.

Particulars

The 24 June 2016 SMR reported on annual win and losses and the amount of cash Customer 44 was prepared to carry.

The 31 January 2018 SMR reported on the cash deposit of $980,000 by an unknown person at the Suncity cash administration desk on 25 January 2018 as pleaded at paragraph 1708.

The 24 February 2020 SMR reported that Customer 44 was an inactive foreign PEP who had experienced significant junket losses, annual individual win and losses and noted Crown's inability to verify Customer 44's source of wealth.

1711. On each occasion that Crown Melbourne formed a suspicion with respect to Customer 44 for the purposes of s41 of the Act, it was required to apply its ECDD program to Customer 44.

Particulars

Rule 15.9(3) of the Rules.

1712. Crown Melbourne did not carry out appropriate risk-based ECDD measures with respect to Customer 44 on each occasion that Crown Melbourne formed a suspicion with respect to Customer 44 for the purposes of s41 of the Act.

a. There are no records of ECDD being conducted following the lodgement of SMRs on 24 June 2016, 31 January 2018 and 24 February 2020: see paragraphs 664 and 685.

b. Appropriate risk-based steps were not taken to obtain or analyse information about Customer 44's source of wealth/funds from an ML/TF perspective: see paragraph 667. The SMR given to the AUSTRAC CEO on 24 February 2020 expressly stated that Crown was unable to verify Customer 44's source of wealth.

c. Appropriate risk-based steps were not taken to analyse and monitor Customer 44's transactions – both past and future – including to understand their economic purpose: see paragraphs 590 and 666.

d. On each occasion that senior management considered whether to continue the business relationship with Customer 44, senior management failed to give adequate consideration to whether the ML/TF risks posed by Customer 44 were within Crown Melbourne or Crown Perth's risk appetite: see paragraph 668ff.

Particulars

Rules 15.9(3), 15.10(1)(c), (d), (2), (5) and (6) of the Rules.

See particulars to paragraph 1709.

1713. At all times from 1 March 2016, Customer 44 was a foreign PEP.

Particulars

Customer 44 was a member of several foreign political bodies.

1714. At all times from 1 March 2016, Crown Melbourne and Crown Perth were required to apply their ECDD program to Customer 44.

Particulars

Rules 15.9(2) and 15.11 of the Rules.

See paragraphs 660, 663 and 666.

1715. Crown Melbourne and Crown Perth did not carry out appropriate risk-based ECDD measures with respect to Customer 44 on and from 1 March 2016 given his status as a foreign PEP. In particular:

a. Crown Melbourne and Crown Perth did not undertake a detailed analysis of Customer 44's KYC information, nor did it take reasonable measures to identify Customer 44's source of wealth/funds;

b. senior management approval for Crown Melbourne and Crown Perth to continue a business relationship with Customer 44 did not give adequate consideration to the ML/TF risks posed by the customer; and

c. senior management approval for Crown Melbourne to continue to provide designated services to Customer 44 did not give adequate consideration to the ML/TF risks posed by the customer.

Particulars

Rules 15.10(2), 15.10(6), 15.11 of the Rules.

See paragraphs 1709 and 1712.

See paragraph 660, 663, 666, 667 and 668.

1716. Between 26 November 2014 and 6 March 2019, Crown Melbourne rated Customer 44 high risk.

Particulars

Crown Melbourne rated Customer 44 high risk on three occasions between 24 June 2016 and 6 March 2019: see paragraph 1705.

1717. On each occasion that Crown Melbourne rated Customer 44 high risk, Crown Melbourne was required to apply its ECDD program to Customer 44.

Particulars

Rule 15.9(1) of the Rules.

See paragraph 661.

1718. Crown Melbourne did not carry out appropriate risk-based ECDD measures with respect to Customer 44 on each occasion that Crown Melbourne rated Customer 44 high risk.

Particulars

See paragraphs 1709, 1712 and 1715.

See paragraphs 661, 666, 667 and 668.

1719. By reason of the matters pleaded from paragraphs 1697 to 1718, on and from 1 March 2016, Crown Melbourne and Crown Perth:

a. did not monitor Customer 44 in relation to the provision of designated services, with a view to identifying, mitigating and managing the ML/TF risks reasonably faced; and

b. did not do so in accordance with rr 15.5 and 15.9 of the Rules.

1720. By reason of the matters pleaded at paragraph 1719, Crown Melbourne and Crown Perth contravened s36(1) of the Act on and from 1 March 2016 with respect to Customer 44.

Particulars

Section 36(1) of the Act is a civil penalty provision: s36(2) of the Act.

Customer 45

1721. Customer 45 has been a customer of Crown Melbourne since 15 February 2018.

1722. From at least 15 February 2018, Crown Melbourne provided Customer 45 with designated services within the meaning of table 1 and table 3, s6 of the Act.

1723. From at least 15 February 2018, Customer 45 received designated services at Crown Melbourne as a junket player, facilitated through one junket operator.

Particulars to paragraphs 1722 and 1723

Customer 45 received designated services as a junket player under the Suncity junket. Crown Melbourne recorded that Customer 45's gaming activity on the Suncity junket programs involved turnover of HKD234,000,000 and AU$52,863,701.

On 26 January 2020, Crown Melbourne opened a DAB account and a safekeeping account for Customer 45.

1724. Customer 45 has been a customer of Crown Perth since 8 August 2017.

1725. From at least 8 August 2017, Crown Perth provided Customer 45 with designated services within the meaning of table 1 and table 3, s6 of the Act.

1726. From at least 8 August 2017, Customer 45 received designated services at Crown Perth as a junket player, facilitated through one junket operator.

Particulars to paragraphs 1725 and 1726

Customer 45 received designated services as a junket player under the Suncity junket. Crown Perth recorded that Customer 45's gaming activity on Suncity junket programs involved turnover of $27,762,000.

On 8 August 2017, Crown Perth opened a DAB account and a safekeeping account for Customer 45.

On 26 January 2020, Crown Perth opened a DAB account and a safekeeping account for Customer 45 under a second PID.

1727. At all relevant times, Customer 45 was a foreign PEP on the basis of a position held in a foreign political organisation since January 2013.

1728. On 21 February 2018, Customer 45 was rated high risk by Crown Melbourne.

Particulars

On various occasions between 21 February 2018 and 21 October 2021, Crown Melbourne assessed Customer 45 as high risk.

See paragraph 481.

1729. At all times on and from 15 February 2018, Customer 45 should have been recognised by Crown Melbourne as a high risk customer as a result of his PEP status pleaded in paragraph 1727.

Particulars

Section 36(1)(a), (b) of the Act and Chapter 15 of the Rules.

1730. At no time was Customer 45 rated high risk by Crown Perth.

1731. At all times on and from 8 August 2017, Customer 45 should have been recognised by Crown Perth as a high risk customer as a result of his PEP status pleaded in paragraph 1727.

Particulars

Section 36(1)(a), (b) of the Act and Chapter 15 of the Rules.

On 27 October 2017, Crown Perth assessed Customer 45 as low risk.

See paragraph 481.

The ML/TF risks posed by Customer 45

1732. On and from 8 August 2017 with respect to Crown Perth, and 15 February 2018 with respect to Crown Melbourne, designated services provided to Customer 45 posed higher ML/TF risks including because the provision of designated services to Customer 45 involved a combination of the following factors:

a. Customer 45 received high value financial (table 1, s6) and gaming services (table 3, s6) provided through multiple junket programs: see paragraph 473ff;

b. Customer 45 was a junket player;

c. Customer 45 was a foreign PEP: see paragraphs 118 and 663;

d. by no later than October 2019, Crown Melbourne recorded that Customer 45's turnover on junket programs at Crown Melbourne had exceeded HKD234,000,000 and AU$52,863,701;

e. by no later than August 2019, Crown Perth recorded that Customer 45's turnover on junket programs at Crown Perth had exceeded $27,762,000;

f. designated services provided to Customer 45 lacked transparency as the services were provided through the channel of junket programs: see paragraph 477(e);

g. the table 3, s6, designated services provided to Customer 45 involved high turnover; and

h. by reason of the matters set out at subparagraphs a. to g. above, there were higher ML/TF risks associated with Customer 45's source of wealth/funds.

Monitoring of Customer 45's transactions

1733. At no time did Crown Melbourne or Crown Perth appropriately monitor Customer 45's transactions on a risk-basis.

Particulars

Section 36(1)(a), (b) of the Act and Rules 15.4 to 15.8 of the Rules.

Crown Melbourne and Crown Perth were unable to monitor the ML/TF risks posed by Customer 45's transactions appropriately because they did not make and keep appropriate records of designated services provided to junket players: see paragraph 483ff.

Crown Melbourne and Crown Perth did not apply appropriate risk-based transaction monitoring to designated services provided to Customer 45: see paragraphs 590ff, 629 to 642 and 643 to 649.

Ongoing customer due diligence

1734. On and from 8 August 2017 with respect to Crown Perth and 15 February 2018 with respect to Crown Melbourne, on multiple occasions, the provision of designated services to Customer 45 by Crown Melbourne and Crown Perth raised red flags reflective of higher ML/TF risks as a result of Customer 45's junket activity.

Particulars

See paragraph 477.

Junket activity in 2017

Between 9 August 2017 and 19 August 2017, Customer 45 was a key player on a Suncity junket program operated by Customer 1 at Crown Perth. Crown Perth recorded that Customer 45's turnover was $27,762,000 with losses of $799,900.

Junket activity in 2018

Between 1 February 2018 and 28 February 2018, Customer 45 was a key player on a Suncity junket program operated by Customer 1 at Crown Melbourne. Crown Melbourne recorded that Customer 45's turnover during this program was approximately HKD234,000,000.

On 17 February 2018, Customer 45 was involved in two disputes in respect of the outcome of play worth $2,250,200 and $1,661,200 while playing baccarat at Crown Melbourne.

On 19 February 2018, Customer 45 was involved in three disputes in respect of the outcome of play worth $1,453,000, $1,289,000 and $1,233,000 while playing baccarat at Crown Melbourne.

On 21 February 2018, Customer 45 was involved in two disputes in respect of the outcome of play worth $1,688,550 and $1,688,550 while playing baccarat at Crown Melbourne.

Junket activity in 2019

Between 1 February 2019 and 28 February 2019, Customer 45 was a key player on a Suncity junket program operated by Customer 1 at Crown Melbourne. Crown Melbourne recorded that Customer 45's turnover was $38,301,025.70 with wins of $778,764.88.

Between 1 October 2019 and 31 October 2019, Customer 45 was a key player on a Suncity junket program operated by Customer 1 at Crown Melbourne. Crown Melbourne recorded that Customer 45's turnover was $14,562,676.46 with losses of $266,721.47.

On 2 October 2019, Customer 45 was involved in a dispute in respect of the outcome of play worth $650,000 while playing baccarat at Crown Melbourne.

On 3 October 2019, Customer 45 was involved in a dispute in respect of the outcome of play worth $925,000 while playing baccarat at Crown Melbourne.

1735. At no time did Crown Melbourne or Crown Perth undertake appropriate risk-based customer due diligence with respect to Customer 45 with a view to identifying, mitigating and managing the ML/TF risks posed by the provision of designated services on and from 8 August 2017 with respect to Crown Perth and 15 February 2018 with respect to Crown Melbourne.

a. At no time did Crown Melbourne or Crown Perth take appropriate steps to understand whether Customer 45's source of wealth/funds was legitimate.

b. At no time did Crown Melbourne or Crown Perth take appropriate steps to identify or analyse the ML/TF risks of Customer 45's transactions or to consider whether they had a lawful purpose.

c. On each occasion that senior management considered whether to continue the business relationship with Customer 45, senior management failed to give adequate consideration to whether the ML/TF risks posed by Customer 45 were within Crown Melbourne or Crown Perth's risk appetite.

Particulars

Section 36(1)(a) of the Act.

The due diligence steps taken with respect to Customer 45 included:

Database searches

On 27 October 2017, the Crown Perth Legal Officer – AML performed a risk intelligence search in respect of Customer 45, which reported that he was a foreign PEP on the basis of a position held in a foreign political organisation since January 2013.

On 20 March 2017, 20 February 2018, 21 February 2019, 26 February 2020 and 24 December 2020, Crown Melbourne performed risk intelligence searches in respect of Customer 45.

On 21 February 2019 and 19 March 2020, Crown Melbourne performed media searches in respect of Customer 45.

None of these steps were proportionate to the ML/TF risks reasonably posed by Customer 45 on and from 8 August 2017 (Crown Perth) and 15 February 2018 (Crown Melbourne).

Senior management engagement (Crown Perth)

On 27 October 2017, the Crown Perth AML Legal Officer sought approval from Crown Perth management, including the Chief Legal Officer (Australian Resorts), the Senior Vice President (International Business) and the Chief Operating Officer (Crown Perth) to continue to conduct a relationship with Customer 45, after a match following risk intelligence searches reported that Customer 45 was a foreign PEP.

On 2 November 2017, the Senior Vice President (International Business) informed the Chief Legal Officer (Australian Resorts) that

he had performed an open source search on Customer 45 but had not located any information to corroborate the information reported in the risk intelligence search results.

On 5 December 2017 and 19 December 2017, the Crown Perth AML Legal Officer repeated the request for approval to continue a business relationship with Customer 45 to the Chief Operating Officer (Crown Perth) and the Chief Legal Officer (Australian Resorts).

None of these steps were proportionate to the ML/TF risks reasonably posed by Customer 45 on and from 8 August 2017.

Senior management engagement (Crown Melbourne)

On 21 February 2018, the Crown Melbourne Group Credit Manager (VIP International) prepared a profile with respect to Customer 45, that noted Customer 45 was in-house at Crown Melbourne playing under a Suncity junket program with recorded turnover of HKD234,000,000 and recommended to allow Customer 45 to attend Crown Melbourne on a cash basis.

On 21 February 2018, this profile was provided to the Senior Vice President (International Business) and the Group General Manager (International Business Operations). The Senior Vice President (International Business) responded indicating that Customer 45 appeared acceptable to him.

On 21 February 2018, the CTRM reported to the Group General Manager (AML), copying the Chief Legal Officer (Australian Resorts), that Customer 45 had been identified as a PEP and sought approval to continue a business relationship and continue providing designated services to the Customer.

On 9 October 2019, CTRM repeated the request for approval from the Chief Legal Officer (Australian Resorts). On 11 October 2019, the Chief Legal Officer (Australian Resorts) approved continuing a business relationship with Customer 45.

Prior to October 2019, none of these steps were proportionate to the ML/TF risks reasonably posed by Customer 45 on and from 15 February 2018.

Enhanced customer due diligence

1736. At all times that Crown Melbourne or Crown Perth provided a designated service to Customer 45, he was a foreign PEP.

Particulars

Section 36(1)(a) of the Act.

1737. At all times that Crown Melbourne and Crown Perth provided a designated service to Customer 45, was required to apply its ECDD program to Customer 45.

Particulars

Rules 15.9(2) and 15.11 of the Rules.

See paragraphs 660, 663 and 666.

1738. Crown Melbourne and Crown Perth did not carry out appropriate risk-based ECDD measures with respect to Customer 45 at all times that they provided a designated service to Customer 45 given his status as a foreign PEP. In particular:

a. Crown Melbourne and Crown Perth did not undertake a detailed analysis of Customer 45's KYC information or analyse the legitimacy of Customer 45's source of wealth/funds;

b. despite multiple requests in 2017 for senior management approval for continuing business relationship with Customer 45 as a foreign PEP, there is no record of any such approval being given; and

c. despite multiple requests in 2017 for senior management approval for continuing to provide designated services to Customer 45 as a foreign PEP, there is no record of any such approval being given.

Particulars

Rules 15.10(2), 15.10(6), 15.11 of the Rules

See paragraph 1735.

See paragraphs 660, 663, 666, 667 and 668.

1739. On and from 21 February 2018, Crown Melbourne rated Customer 45 high risk.

Particulars

Between 21 February 2018 and 12 October 2021, Crown Melbourne rated Customer 45's risk to be high on four occasion: see paragraph 1728.

1740. On each occasion that Crown Melbourne rated Customer 45 high risk, Crown Melbourne was required to apply its ECDD program to Customer 45.

Particulars

Rule 15.9(1) of the Rules.

See paragraph 661.

1741. Crown Melbourne did not carry out appropriate risk-based ECDD measures with respect to Customer 45 on each occasion that Crown Melbourne rated Customer 45 high risk.

Particulars

At no time did Crown Melbourne conduct ECDD following each occasion that it rated Customer 45 high risk.

See paragraph 1735.

See paragraphs 661, 666, 667 and 668.

1742. By reason of the matters pleaded from paragraphs 1721 to 1741, on and from 15 February 2018, Crown Melbourne:

a. did not monitor Customer 45 in relation to the provision of designated services, with a view to identifying, mitigating and managing the ML/TF risks reasonably faced; and

b. did not do so in accordance with rr 15.5 and 15.9 of the Rules.

1743. By reason of the matters pleaded at paragraph 1742, Crown Melbourne contravened s36(1) of the Act on and from 15 February 2018 with respect to Customer 45.

Particulars

Section 36(1) of the Act is a civil penalty provision: s36(2) of the Act.

1744. By reason of the matters pleaded from paragraphs 1721 to 1741, on and from 8 August 2017, Crown Perth:

a. did not monitor Customer 45 in relation to the provision of designated services, with a view to identifying, mitigating and managing the ML/TF risks reasonably faced; and

b. did not do so in accordance with rr 15.5 and 15.9 of the Rules.

1745. By reason of the matters pleaded at paragraph 1744, Crown Perth contravened s36(1) of the Act on and from 8 August 2017 with respect to Customer 45.

Particulars

Section 36(1) of the Act is a civil penalty provision: s36(2) of the Act.

Customer 46

1746. Customer 46 was a customer of Crown Melbourne between 9 June 1993 and 15 July 2016.

Particulars

On 15 July 2016, Customer 46 self-excluded himself from gaming services at Crown Melbourne.

1747. From at least December 2006 to 22 January 2021, Crown Melbourne provided Customer 46 with designated services within the meaning of table 1 and table 3, s6 of the Act.

Particulars

On 24 September 1996, Crown Melbourne opened a CCF account (AUD) in respect of Customer 46. On 7 June 2009, Crown Melbourne closed this CCF account.

On 14 June 2006, Crown Melbourne opened a DAB account and a safekeeping account (AUD) in respect of Customer 46, which remains open.

On 7 June 2009, Crown Melbourne opened a credit facility (AUD) in respect of Customer 46. On 10 June 2013, Crown Melbourne closed this credit facility.

Between 1996 and 10 May 2016, Customer 46 had a cumulative individual loss of $57,452,810.

On 22 January 2021, Crown Melbourne issued a WOL in respect of Customer 46.

As at 19 January 2022, Customer 46 had a Crown Melbourne DAB account balance of $8,792. Customer 46's Crown Melbourne DAB account balance had not changed since at least 1 August 2020.

1748. From at least December 2006 to April 2016, Customer 46 received designated services from Crown Melbourne as a junket player, facilitated through five different junket operators.

Particulars

Customer 46 received designated services through the Suncity, Chinatown and three other junkets.

By 13 October 2014, Crown Melbourne recorded Customer 46's individual gaming activity and gaming activity on junket programs as cumulative turnover of $1,414,682,854 with a cumulative loss of $41,931,786.

The ML/TF risks posed by Customer 46

1749. By 1 March 2016, higher ML/TF risks were indicated by the nature and purpose of Customer 46's business relationship with Crown Melbourne, the nature of the transactions he had been conducting, together with the suspicions Crown Melbourne itself had formed with respect to Customer 46.

Particulars

Section 36(1)(a), (b) of the Act and Chapter 15 of the Rules.

Customer 46 was a junket player. He received designated services through the channel of junket programs. This channel lacked transparency: see paragraph 477.

SMRs by 1 March 2016

By 1 March 2016, Crown Melbourne had given the AUSTRAC CEO 38 SMRs in relation to Customer 46 – on 20 February 2006, 22 February 2006, 6 March 2006, 6 April 2006, 7 April 2006, 19 April 2006, 9 August 2006, 5 January 2007, 20 February 2007, 18 May 2007, 8 June 2007, 26 June 2007, 23 January 2008, 11 February 2008, 9 May 2008, 24 July 2008, 30 September 2008, 3 February 2009, 13 February 2009, 19 February 2009, 24 February 2009, 5 June 2009, 25 June 2009, 6 July 2009, 14 January 2010, 25 June 2010, 29 December 2010, 28 January 2011, 25 March 2011, 9 May 2011, 12 July 2011, 12 April 2013, 12 July 2013, 17 October 2013, 27 March 2014, 24 April 2014, 26 May 2014 and 8 October 2014. The SMRs reported Customer 46's significant annual individual and junket losses, attempts by Customer 46 to avoid the $10,000 transaction threshold, increases in average bet, international transactions to and from a corporate account, large cash transactions, associations with other Crown Melbourne patrons, third party transactions and the amount of cash Customer 46 was prepared to carry.

From time to time, the SMRs identified another patron associated with Customer 46 that Crown Melbourne understood to be

Customer 46's wife. Crown Melbourne recorded that patron's cumulative losses between 2001 and 2015 to be $2,032,013.

Law enforcement enquiries by 1 March 2016

On 23 February 2011, 27 July 2011 and 24 July 2014, Crown Melbourne received LEA enquiries in respect of Customer 46.

Gaming activity by 1 March 2016

On 24 April 2014, Customer 46 was a key player in a Chinatown junket program operated by Customer 11. Crown Melbourne recorded Customer 46's losses under the junket program as $3,006,640.

By 13 October 2014, Customer 46 had attended 69 programs. By 13 October 2014, Crown Melbourne recorded Customer 46's individual gaming activity and gaming activity on junket programs as cumulative turnover of $1,414,682,854 with a cumulative loss of $41,931,786. The total historical commission paid to him was $8,387,676.

Credit facilities by 1 March 2016

On 11 June 2010, a Crown Senior Vice President in the international business team recommended that Crown Melbourne approve a credit of $500,000 on a one off basis for Customer 46. Customer 46 was described by the Senior Vice President to be extremely well linked to a foreign government and military. Crown Melbourne approved the credit limit.

In 2011, Customer 46 owed Crown Melbourne a debt of $2,499,823.

Between 7 June 2009 and 10 June 2013, Customer 46 was granted credit at Crown Melbourne with limits ranging from $10,000 to $2,500,000. Crown obtained Central Credit Gaming Reports throughout the period. Crown Melbourne added special conditions requiring funds to be repaid by certain dates. The provision of designated services to Customer 46 in the form of credit facilities was considered in light of, or approved/denied as a result of, Crown Melbourne's confidence in Customer 46's ability to repay any debt incurred and not ML/TF risk. On 10 June 2013, Customer 46 had his credit facility cancelled.

Large and unusual telegraphic transfers by 1 March 2016

Customer 46 was involved in large and unusual telegraphic transfers, which included:

- between 24 June 2010 and 5 January 2016, Customer 46 transferred AU$24,750,069 into his Crown DAB account, including six large foreign currency transactions;
- between 9 July 2011 and 14 January 2016, Customer 46 transferred AU$2,072,618 from his Crown DAB account to his

personal account, including two large foreign currency transactions;

- in 2010, Customer 46 transferred $1,452,263 from his Crown Melbourne DAB account to his Crown Perth DAB account;
- in 2011, Customer 46 transferred $10,000 from his Crown Perth DAB account to his Crown Melbourne DAB account;
- between September 2008 and July 2015, Customer 46 received approximately $2,567,618 from third parties, $7,034,771 from third party companies, $1,005,057 from a Crown group entity and $1,687,612 from another Australian casino. The third parties included Company 14, which had also sent substantial telegraphic transfers to Customer 33 and Customer 4;
- between July 2013 and April 2014, Customer 46 transferred from his DAB account $3,635,087 to a foreign casino, $2,185,078 to a second foreign casino and $940,000 to a Crown group entity; and
- on 18 June 2014, Customer 46 transferred from his DAB account $3,500,000 to a junket operator: SMR dated 29 November 2021.

Due diligence conducted by 1 March 2016

On various occasions between 5 February 2009 and 13 October 2014, Crown Melbourne prepared a credit patron profile in respect of Customer 46 for the purpose of assessing his creditworthiness.

1750. As at 1 March 2016, Customer 46 should have been recognised by Crown Melbourne as a high risk customer for the reasons pleaded at paragraph 1749.

1751. It was not until 20 January 2021 that Customer 46 was rated high risk by Crown Melbourne.

Particulars

On various occasions between 11 February 2008 and 28 January 2011 and between 8 July 2016 and 18 February 2020, Crown Melbourne assessed Customer 46 as moderate risk.

On various occasions between 23 February 2011 and 8 October 2014, Crown Melbourne rated Customer 46 as significant risk.

Crown Melbourne first assessed Customer 46's risk to be high on 20 January 2021, nearly five years after he self-excluded himself from gaming activity at Crown Melbourne and Crown Perth. Customer 46 was also assessed and rated high risk on 27 July 2021.

This was despite Customer 46's numerous large third party transactions and that 38 SMRs were given to the AUSTRAC CEO in respect of Customer 46 by 1 March 2016.

See paragraph 481.

1752. At all times on and from 1 March 2016, Customer 46 should have been recognised by Crown Melbourne as a high risk customer by reason of the matters pleaded at paragraphs 1749, 1753, 1755, 1756, 1757, 1759 and 1762.

Particulars

Section 36(1)(a), (b) of the Act and Chapter 15 of the Rules.

1753. On and from 1 March 2016, designated services provided to Customer 46 posed higher ML/TF risks including because the provision of designated services to Customer 46 involved a combination of the following factors:

a. Customer 46 was a foreign PEP: see paragraphs 118 and 663;

b. Customer 46 was a junket player;

c. Customer 46 received high value financial (table 1, s6) and gaming services (table 3, s6) provided through junket programs: see paragraph 473ff;

d. designated services provided to Customer 46 lacked transparency as the services were provided through the channel of junket programs: see paragraph 477(e);

e. Customer 46 played on Suncity and Chinatown junkets;

f. by May 2016, Crown Melbourne recorded Customer 46's individual rated gaming activity as a cumulative individual loss of $57,452,810;

g. these transactions took place against the background of:

i. designated services provided to Customer 46 by 1 March 2016 involved large cross-border movements of funds and telegraphic transfers from third parties;

ii. law enforcement having expressed an interest in Customer 46 in February 2011 and July 2014;

iii. by 13 October 2014, Crown Melbourne recorded Customer 46's individual gaming activity and gaming activity on junket programs as cumulative turnover of $1,414,682,854 with a cumulative loss of $41,931,786;

iv. 38 SMRs being given to the AUSTRAC CEO by Crown Melbourne by 1 March 2016;

h. by 1 March 2016, Crown Melbourne were aware that Customer 46 was well connected to both a foreign government and a foreign military;

i. Customer 46 was known to be a very close associate of Person 41, Customer 26 and other individuals associated with or running junkets;

j. despite Customer 46's self-exclusion on 15 July 2016, he continued to attend Crown Melbourne together with his wife in circumstances where Crown Melbourne had suspicions that at least one of Customer 46's wife's transactions were made on behalf of Customer 46;

k. in July 2019, Crown Melbourne was aware that Customer 46 was identified in several media reports as a close associate to a foreign PEP and a person with ties to organised crime, as a person who had been investigated for corruption in a foreign country and as a person who had been on board of a private jet that had been searched by a law enforcement agency in connection with money laundering; and

l. by reason of the matters set out at subparagraphs a. to k. above, there were real risks that Customer 46's source of wealth and source of funds were not legitimate.

Monitoring of Customer 46's transactions

1754. At no time did Crown Melbourne appropriately monitor Customer 46's transactions on a risk-basis.

Particulars

Section 36(1)(a), (b) of the Act and Rules 15.4 to 15.8 of the Rules.

Crown Melbourne was unable to monitor the ML/TF risks posed by Customer 46's transactions appropriately because it did not make and keep appropriate records of designated services provided to junket players: see paragraph 483ff.

Crown Melbourne did not apply appropriate risk-based transaction monitoring to designated services provided to Customer 46: see paragraphs 590ff, 629 to 642 and 643 to 649.

Customer 46's transactions involved transactions indicative of ML/TF vulnerabilities that were not detected prior to a 2021 lookback. Had appropriate risk-based transaction monitoring been applied, these transactions could have been identified earlier: see paragraphs 686 and 687.

In 29 November 2021, an SMR was given to the AUSTRAC CEO in connection with a junket operator active at Crown Melbourne until 2017 who was issued with a WOL on 15 June 2021. Relevantly, Crown Melbourne identified that on 18 June 2014 Customer 46 transferred $3,500,000 to the junket operator. Customer 46 was noted as having played under a Chinatown junket operated by Customer 11 who was the recipient of the transfer. Customer 46 was noted as being a foreign PEP and a relative of a foreign PEP.

Ongoing customer due diligence

1755. On and from 1 March 2016, on multiple occasions, the provision of designated services to Customer 46 by Crown Melbourne raised red flags reflective of higher ML/TF risks as a result of his gaming activity, which involved large buy-ins.

Particulars

See paragraph 477.

Gaming activity in 2016

On 29 March 2016, Customer 46 received a telegraphic transfer of $50,000 from a third party.

In April 2016, Customer 46 participated in a junket program.

On 2 April 2016, Customer 46 transferred $150,000 into his DAB account.

On 5 April 2016, Customer 46 transferred $130,000 from his DAB account to his personal account.

By 15 July 2016, Crown Melbourne recorded Customer 46's 2016 individual rated gaming activity to be a buy-in of $2,323,900 with a loss of $81,340.

On 15 July 2016, Customer 46 self-excluded himself from gaming services at Crown Melbourne and Crown Perth.

1756. In 2019, Crown Melbourne became aware of media articles detailing allegations that Customer 46 had faced corruption charges and had been the subject of law enforcement suspicion in respect of money laundering.

Particulars

In July 2019, Crown Melbourne were aware of media reports which identified that:

- Customer 46 was related to a foreign PEP;
- Customer 46 had faced serious corruption allegations in a foreign country; and
- in 2016, Customer 46 had been aboard a private jet together with another Crown Melbourne high-roller Person 41 when it was searched by a law enforcement agency on suspicion of international money laundering.

Sometime after October 2019, publicly accessible reports identified Customer 46 to have been investigated by Australian AML authorities, and that he was associated with a company that was allegedly used by casino gamblers and suspected organised-crime figures to transfer hundreds of millions of dollars in and out of Australia. There is no evidence that these reports came to Crown Melbourne's attention as part of their due diligence process.

A February 2020 media report directly concerned Customer 46's activities in respect of casinos. The media report identified that Customer 46 reportedly flew to Vanuatu together with a junket operator Person 41 for the purpose of investigating casinos for purchase. There is no evidence that these reports came to Crown Melbourne's attention as part of their due diligence process.

1757. From 15 July 2016, Crown Melbourne failed to satisfy itself as to whether it was providing designated services to Customer 46 or his wife, raising red flags reflective of higher ML/TF risks.

Particulars

On 22 February 2006, an SMR given to the AUSTRAC CEO by Crown Melbourne in respect of Customer 46 stated that Customer 46's wife did not have the rated play to justify her transactions, and that it was possible that the gaming chips presented by her were Customer 46's.

On 15 July 2016, Customer 46 self-excluded himself from gaming services at Crown Melbourne and Crown Perth.

After Customer 46 self-excluded from Crown Melbourne and Crown Perth, his wife continued to engage in gaming activity at Crown Melbourne. Between 2016 and 2020, Customer 46's wife recorded a cumulative win of $150,201.

On 23 June 2017, despite Customer 46's self-exclusion from gaming activity at Crown Melbourne and Crown Perth, Customer 46 attended Crown Melbourne together with his wife.

On 18 February 2020, Customer 46's wife contacted Crown Melbourne and requested that her gaming activity not be rated while playing in the Mahogany room. Customer 46's wife identified the reason for the request as a desire to maintain a low profile: SMR dated 18 February 2020.

Crown Melbourne failed to satisfy itself that it was providing designated services to Customer 46's wife only, and not also to Customer 46 himself.

1758. At no time did Crown Melbourne undertake appropriate risk-based customer due diligence with respect to Customer 46 with a view to identifying, mitigating and managing the ML/TF risks posed by the provision of designated services on and from 1 March 2016.

a. At no time did Crown Melbourne take appropriate steps to understand whether Customer 46's source of wealth/funds was legitimate.

b. At no time did Crown Melbourne take appropriate steps to identify or analyse the ML/TF risks of Customer 46's transactions or to consider whether they had a lawful purpose.

c. At no time did Crown Melbourne give appropriate consideration to whether large and high risk transactions should be processed.

d. Prior to the decision to issue Customer 46 with a WOL in January 2021, there is no record of senior management considering whether continuing the business relationship with Customer 46 was within Crown Melbourne's ML/TF risk appetite in light of the ML/TF risks posed by Customer 46: see paragraph 668ff.

Particulars

Section 36(1)(a) of the Act.

The due diligence steps taken with respect to Customer 46 included:

- in July 2019, in response to a media report identifying Customer 46 and a number of other patrons, Crown Melbourne collated the available internal information relating to Customer 46;
- in July 2019 and May 2021, Crown Melbourne conducted risk intelligence and media searches in respect of Customer 46; and
- by February 2020, Crown Melbourne had been unable to identify any information regarding Customer 46's source of funds/wealth beyond the fact that he was chairman of two foreign companies: SMR dated 18 February 2020.

None of these steps were proportionate to the ML/TF risks reasonably posed by Customer 46 on and from 1 March 2016.

On 22 January 2021, Crown Melbourne issued a WOL in respect of Customer 46 following a decision from the POI Committee as a result of references to Customer 46 in the ILGA matter.

Enhanced customer due diligence

1759. Having formed a suspicion for the purposes of s41 of the Act, Crown Melbourne gave the AUSTRAC CEO SMRs with respect to Customer 46 on:

a. 23 June 2017; and

b. 18 February 2020.

Particulars

The 23 June 2017 SMR reported Customer 46's and his wife's annual losses together with the amount of cash that Customer 46 and his wife were prepared to carry.

The 18 February 2020 SMR reported Customer 46's annual losses given Crown Melbourne's inability to verify his source of wealth/funds, Customer 46's association with a high-profile foreign PEP and Customer 46's wife's request to Crown Melbourne that her play in the Mahogany Room not be rated.

1760. On each occasion that Crown Melbourne formed a suspicion with respect to Customer 46 for the purposes of s41 of the Act, it was required to apply its ECDD program to Customer 46.

Particulars

Rule 15.9(3) of the Rules.

1761. Crown Melbourne did not carry out appropriate risk-based ECDD measures with respect to Customer 46 on each occasion that Crown Melbourne formed a suspicion with respect to Customer 46 for the purposes of s41 of the Act.

a. There are no records of ECDD being conducted following the lodgement of the SMR on 23 June 2017.

b. Appropriate risk-based steps were not taken to obtain or analyse information about Customer 46's source of wealth/funds: see paragraph 667.

c. Prior to the decision to issue Customer 46 with a WOL in January 2021, there is no record of senior management considering whether continuing the business relationship with Customer 46 was within Crown Melbourne's ML/TF risk appetite in light of the ML/TF risks posed by Customer 46. On 15 July 2016, Customer 46 self-excluded himself from gaming services at Crown Melbourne.

Particulars

Rules 15.9(3), 15.10(1)(c), (d), (2), (5) and (6) of the Rules.

Following the lodgement of the 18 February 2020 SMR, Crown Melbourne obtained a risk intelligence report in respect of Customer 46 and his wife. The report identified Customer 46 to be a relative or close associate of a foreign PEP.

See particulars to paragraph 1758.

1762. At all times from 1 March 2016, Customer 46 was a foreign PEP.

Particulars

Customer 46 was a foreign PEP on the basis that Customer 46 was a relative or close associate of a foreign PEP.

Media reports in 2019 identified Customer 46's status as a PEP by association.

On 18 February 2020, Crown Melbourne obtained a risk intelligence search that identified Customer 46 as a foreign PEP.

It was not until 11 March 2021 that Crown Melbourne first determined Customer 46 to be a foreign PEP.

1763. At all times from 1 March 2016, Crown Melbourne was required to apply its ECDD program to Customer 46.

Particulars

Rules 15.9(2) and 15.11 of the Rules.

See paragraphs 660, 663 and 666.

1764. Crown Melbourne did not carry out appropriate risk-based ECDD measures with respect to Customer 46 on and from 1 March 2016 given his status as a foreign PEP. In particular:

a. Crown Melbourne did not undertake a detailed analysis of Customer 46's KYC information, nor did it take reasonable measures to identify Customer 46's source of wealth/funds;

b. no steps were taken to seek and obtain senior management approval for continuing a business relationship with Customer 46 having regard to the ML/TF risks posed by the customer;

c. no steps were taken to seek and obtain senior management approval for whether Crown Melbourne should continue to provide designated services to Customer 46. On 15 July 2016, Customer 46 self-excluded himself from gaming services at Crown Melbourne.

Particulars

Rules 15.10(2), 15.10(6), 15.11 of the Rules.

See paragraphs 1758 and 1761.

Until 2019, no due diligence was conducted in respect of Customer 46. Searches conducted in 2019 were in response to media articles and did not seek to identify, mitigate and manage the ML/TF risk related to Customer 46's status as a foreign PEP.

See paragraphs 660, 663, 666, 667 and 668.

1765. By reason of the matters pleaded from paragraphs 1746 to 1764, on and from 1 March 2016, Crown Melbourne:

a. did not monitor Customer 46 in relation to the provision of designated services, with a view to identifying, mitigating and managing the ML/TF risks reasonably faced; and

b. did not do so in accordance with rr 15.5 and 15.9 of the Rules.

1766. By reason of the matters pleaded at paragraph 1765, Crown Melbourne contravened s36(1) of the Act on and from 1 March 2016 to January 2021 with respect to Customer 46.

Particulars

Section 36(1) of the Act is a civil penalty provision: s36(2) of the Act.

Customer 47

1767. Customer 47 was a customer of Crown Melbourne from June 2012 to December 2019.

1768. From at least June 2012 to December 2019, Crown Melbourne provided Customer 47 with designated services within the meaning of table 1 and table 3, s6 of the Act.

Particulars

On 22 June 2012, Crown Melbourne opened a DAB account and a safekeeping account (AUD) for Customer 47, which were closed on 11 November 2021.

Customer 47 played in the Mahogany room on a number of occasions, which is open to Platinum and Black tier customers, and Gold tier customers by invitation.

On 21 July 2015, Crown Melbourne opened a CCF account (AUD) for Customer 47. On 22 July 2015, Crown Melbourne approved a CCF (AUD) for Customer 47 with a credit limit of $500,000. The CCF was closed on 31 December 2015.

Between 2012 and 2015, Crown Melbourne recorded Customer 47's individual rated gaming activity to be a cumulative buy-in $133,752,273 with a cumulative loss of $5,382,113. Customer 47's buy-in escalated significantly from $1,166,247 in 2012 to $85,836,300 in 2015.

Between 2016 and 2019, Crown Melbourne recorded Customer 47's individual rated gaming activity to be a cumulative buy-in of $36,734,590 with a cumulative loss of $5,381,250.

On 19 November 2019, Crown Melbourne issued a WOL in respect of Customer 47.

1769. Customer 47 was a customer of Crown Perth from 26 June 2013 to 15 September 2021.

1770. From at least 4 July 2013, Crown Perth provided Customer 47 with designated services within the meaning of table 1 and table 3, s6 of the Act.

Particulars

On 4 July 2013 Crown Perth opened a DAB account and a safekeeping account (AUD) for Customer 47.

On 11 July 2015, Crown Perth opened a CCF (AUD) for Customer 47, with a credit limit of $250,000 with a TTO of $250,000. On 16 August 2016, Crown Perth closed Customer 47's CCF.

On 25 November 2015, Crown Perth opened a second DAB account and safekeeping account (AUD) for Customer 47 under the same PID as Customer 47's DAB account with Crown Melbourne.

On 15 September 2021, Crown Perth issued an NRL in respect of Customer 47.

The ML/TF risks posed by Customer 47

1771. By 1 March 2016, higher ML/TF risks were indicated by the nature and purpose of Customer 47's business relationship with Crown Melbourne, the nature of the transactions he had been conducting, together with the suspicions Crown Melbourne itself had formed with respect to Customer 47.

Particulars

Section 36(1)(a), (b) of the Act and Chapter 15 of the Rules.

SMRs by 1 March 2016

By 1 March 2016, Crown Melbourne had given the AUSTRAC CEO 11 SMRs in relation to Customer 47 – on 19 September 2012, 12 December 2012, 27 February 2013, 24 May 2013, 23 July 2013, 27 September 2013, 11 February 2014, 13 August 2014, 24 November 2014, 30 December 2014, 5 May 2015. The SMRs described Customer 47's yearly buy-ins, average bets and losses. The grounds of suspicion were based on annual losses and the amount of cash Customer 47 was prepared to carry.

Law enforcement request in 2013

On 26 February 2013, a law enforcement agency requested information from Crown Melbourne relating to Customer 47.

Large and suspicious gaming activity by 1 March 2016

In 2012, Crown Melbourne recorded Customer 47's individual rated gaming activity to be a buy-in of $1,116,247 with a loss of $371,797 and an average bet of $578.

In 2013, Crown Melbourne recorded Customer 47's individual rated gaming activity as escalating to be a buy-in of $6,233,176 with a loss of $1,503,956 and an average bet of $2,190.

From 6 November to 21 November 2014, Customer 47 played on a program at Crown Melbourne. Customer 47 staked $300,000 as front money and won approximately $1,170,000. At settlement, Customer 47 requested $150,000 be sent to Crown Perth via telegraphic transfer and the remaining $1,050,000 be provided to him in cash. When he was offered a telegraphic transfer or Crown cheque as an alternative to cash, Customer 47 refused and said that he did not want to have a paper or audit trail. On 24 November 2014, Crown Melbourne gave the AUSTRAC CEO an SMR in respect of Customer 47 relating to this conduct.

In 2014, Crown Melbourne recorded Customer 47's individual rated gaming activity as further escalating to be a buy-in of $40,516,550 with a loss of $1,039,505 and an average bet of $7,050.

In 2015, Crown Melbourne recorded Customer 47's individual rated gaming activity as further escalating to be a buy-in of $85,836,300 with a loss of $2,466,855 and an average bet of $16,240.

Transactions indicative of ML/TF typologies by 1 March 2016

In 2014 and 2015, Customer 47 engaged in transactions indicative of ML/TF typologies involving quick turnover of chips at Crown Melbourne:

- on 23 November 2014, depositing $87,000 in cash and then withdrawing $5,000 cash on the same day, then withdrawing a further $344,310 the following day by telegraphic transfer and $10,000 in cash; and
- on 17 July 2015, depositing by telegraphic transfer $493,620 and then withdrawing $493,620 by telegraphic transfer on the same day.

Due diligence conducted by 1 March 2016

On 22 July 2015, Crown Melbourne obtained information as to Customer 47's occupation, being an occupation that was not fully consistent with, or did not fully support, his source of funds.

1772. By 1 March 2016, higher ML/TF risks were indicated by the nature and purpose of Customer 47's business relationship with Crown Perth.

Particulars

On 22 July 2015, Crown Perth approved an application for a CCF for Customer 47 with a credit limit of $250,000 with a TTO of $250,000. In assessing the application, Crown Perth considered Customer 47's history of play, including at both Crown Perth and Crown Melbourne. Information obtained by Crown Perth as to Customer 47's occupation, was not fully consistent with, or did not fully support, his source of funds across both casinos.

1773. As at 1 March 2016, Customer 47 should have been recognised by Crown Melbourne as a high risk customer for the reasons pleaded at paragraph 1771.

Particulars

Crown Melbourne did not assess Customer 47's risk as high until 26 August 2021, shortly before a WOL was issued.

On various occasions between 19 September 2012 and 25 February 2013, Crown Melbourne rated Customer 47's risk as moderate.

On various occasions between 26 February 2013 and 30 December 2014, Crown Melbourne rated Customer 47's risk as significant.

On various occasions between 11 February 2015 and 25 August 2021, Crown Melbourne rated Customer 47's risk as moderate.

This was despite the 2013 law enforcement inquiry made in respect of Customer 47, Customer 47's escalating individual rated gaming activity and Customer 47's express statement that he did not want there to be a paper or audit trail in respect of his gaming activity.

See paragraph 120.

1774. As at 1 March 2016, there was no basis for Customer 47 to have been rated low risk by Crown Perth for the reasons pleaded at paragraph 1772.

Particulars

At no time did Crown Perth assess the risk of Customer 47 and he was therefore rated low by default: see paragraph 120.

1775. At all times on and from 1 March 2016, Customer 47 should have been recognised by Crown Melbourne and Crown Perth as a high risk customer by reason of the matters pleaded at paragraphs 1771, 1772, 1776, 1777, 1778 and 1780.

Particulars

Section 36(1)(a), (b) of the Act and Chapter 15 of the Rules.

1776. On and from 1 March 2016 designated services provided to Customer 47 posed higher ML/TF risks including because the provision of designated services to Customer 47 involved a combination of the following factors:

a. Customer 47 received high value financial (table 1, s6) and gaming services (table 3, s6);

b. by 2019, Crown Melbourne recorded Customer 47's individual rated gaming activity to be a cumulative turnover of $170,486,863 with a loss of $10,763,363;

c. at various times, Customer 47 had significant parked or dormant funds in his DAB accounts: see paragraph 252;

d. Customer 47 carried and transacted in large cash values;

e. large values were transferred to and from Customer 47's bank accounts and his DAB account, and to and from other customers' DAB accounts, involving the provision by Crown Melbourne of designated services within the meaning of items 31 and 32, table 1, s6 of the Act: see paragraph 411ff;

f. Customer 47 engaged in other transactions indicative of ML/TF typologies and vulnerabilities at Crown Melbourne and Crown Perth, including quick turnover (without betting) and redemption of chips not commensurate with his play;

g. these transactions took place against the background of:

   i. law enforcement having expressed an interest in Customer 47 in 2013;

   ii. 12 SMRs being given to the AUSTRAC CEO by Crown Melbourne by 1 March 2016;

h. in 2019, a cheque presented to Crown Melbourne by Customer 47 was reported as stolen;

i. in July 2016, August 2017, April 2018 and October 2019, Crown Melbourne senior management determined that a business relationship with Customer 47 was beyond its

ML/TF risk appetite and issued Customer 47 with a WOL. However, in September 2016, February 2018 and April 2019, Crown Melbourne senior management determined that a business relationship with Customer 47 was within its risk appetite and revoked the WOL issued in respect of him; and

j. by reason of the matters set out at subparagraphs a. to i. above, there were real risks that Customer 47's source of wealth and source of funds were not legitimate.

Monitoring of Customer 47's transactions

1777. At no time did Crown Melbourne or Crown Perth appropriately monitor Customer 47's transactions on a risk-basis.

Particulars

Section 36(1)(a), (b) of the Act and Rules 15.4 to 15.8 of the Rules.

Crown Melbourne and Crown Perth did not apply appropriate risk-based transaction monitoring to designated services provided to Customer 47: see paragraphs 590ff and 629 to 642.

Customer 47's transactions involved repeated transactions indicative of ML/TF typologies and vulnerabilities that were not detected prior to a 2021 lookback. Had appropriate risk-based transaction monitoring been applied, these transactions could have been identified earlier: see paragraphs 686 and 687.

Transactions indicative of ML/TF typologies – quick turnover (without betting)

Transactions involving Customer 47 were identified as indicative of the ML/TF typology of quick turnover (without betting) at Crown Melbourne by an independent auditor in 2021:

- on 6 July 2016, Customer 47 was credited $20,000 by telegraphic transfers. On 7 July 2016, Customer 47 was debited $60,000 by telegraphic transfer;
- on 30 June 2017, Customer 47 was credited $20,000 and $10,000 by telegraphic transfer. On 1 July 2017, Customer 47 withdrew $81,180 in cash; and
- on 24 April 2018, Customer 47 was credited $50,000 in cash and then debited $50,000 by telegraphic transfer and $15,650 by cash.

Transactions indicative of ML/TF typologies – redemption of chips not commensurate with play

Transactions involving Customer 47 were identified as indicative of the ML/TF typology of redemption of chips not commensurate with play by an independent auditor in 2021:

- on 5 January 2017, Customer 47 cashed $24,000 in chips at Crown Perth and then withdrew $10,000 and $15,000 in CPVs; and

- on 7 July 2017, Customer 47 cashed $75,000 in chips at Crown Melbourne and then withdrew $25,000 and $50,000 in CPVs.

Transactions indicative of ML/TF typologies – parked funds

As at 30 April 2021, Customer 47 had a Crown Melbourne DAB account balance of $269,786 on 30 April 2021 that had been dormant for 505 days. The report stated that the balance was held by Crown on the basis that Customer 47 had an outstanding debt owed to Crown.

Other suspicious transactional activity

An independent auditor in 2021 made the following observations in relation to Customer 47:

- Customer 47 was one of 11 patrons identified as responsible for 66% of the total value of identified quick turnover transactions (the 11 patrons accounted for 22% of the total instances of identified quick turnover transactions);
- on at least one occasion, the total value of chips redeemed by Customer 47 exceeded the total of buy-in value within a 48-hour period without sufficient gaming winnings to justify the additional chips redeemed. On 6 and 7 July 2016, Customer 47 withdrew 300% more than his original deposit. On 30 June 2017 and 1 July 2017, Customer 47 withdrew 271% more than his original deposit. On 24 April 2018, Customer 47 withdrew 131% more than his original deposit; and
- Customer 47 was identified as having sent telegraphic transfers to either a common beneficiary. On 19 March 2016, Customer 47 sent $125,000 to an Australian casino. On 28 March 2016, Customer 47 sent $75,000 to the Australian casino. On 11 June 2017, Customer 47 sent $40,000 to the Australian casino.

Ongoing customer due diligence

1778. On and from 1 March 2016, on multiple occasions, the provision of designated services to Customer 47 by Crown Melbourne and Crown Perth raised red flags reflective of higher ML/TF risks by reason of:

a. Customer 47 engaging in large and unusual transactions; and

b. Customer 47's gaming activity.

Particulars

See paragraph 450 and 451.

Large and unusual transactions

On 13 July 2016, Customer 47 made a cash buy-in at Crown Melbourne of $16,900.

On 30 July 2019, Customer 47 made a cash deposit of $3,000 into his DAB account at Crown Melbourne.

On 26 September 2019, Customer 47 presented a $300,000 cheque and requested it be deposited into his account for gaming purposes. The cheque was accepted, but when Crown Melbourne attempted to bank it the cheque was returned as reported lost or stolen: SMR dated 16 October 2019.

On 16 October 2019, Customer 47 transferred $15,000 from his personal account to his DAB account at Crown Melbourne.

Individual rated gaming activity

In 2016, Crown Melbourne recorded Customer 47's individual rated gaming activity to be a buy-in of $23,246,595 with a loss of $2,135,910.

In 2017, Crown Melbourne recorded Customer 47's individual rated gaming activity to be a buy-in of $5,460,195 with a loss of $1,129,740.

In 2018, Crown Melbourne recorded Customer 47's individual rated gaming activity to be a buy-in of $1,094,545 with a loss of $87,500.

In 2019, Crown Melbourne recorded Customer 47's individual rated gaming activity to be a buy-in of $6,933,255 with a loss of $2,028,100.

1779. At no time did Crown Melbourne or Crown Perth undertake appropriate risk-based customer due diligence with respect to Customer 47 with a view to identifying, mitigating and managing the ML/TF risks posed by the provision of designated services on and from 1 March 2016.

a. At no time did Crown Melbourne or Crown Perth take appropriate steps to understand whether Customer 47's source of wealth/funds was legitimate.

b. At no time did Crown Melbourne or Crown Perth take appropriate steps to identify or analyse the ML/TF risks of Customer 47's transactions or to consider whether they had a lawful purpose.

c. At no time did Crown Melbourne and Crown Perth give appropriate consideration to whether large and high risk transactions should be processed.

d. In July 2016, August 2017, April 2018 and October 2019, Crown Melbourne senior management determined that a business relationship with Customer 47 was outside of its ML/TF risk appetite and issued Customer 47 with a WOL. However, in September 2016, February 2018 and April 2019, Crown Melbourne senior management determined that a business relationship with Customer 47 was within its risk appetite and revoked the WOL issued in respect of him. This was despite the ML/TF risks posed by Customer 47.

e. Prior to the decision to issue Customer 47 with an NRL in September 2021, there is no record of senior management considering whether continuing the business relationship with Customer 47 was within Crown Perth's ML/TF risk appetite in light of the ML/TF risks posed by Customer 47.

Particulars

Section 36(1)(a) of the Act.

Database searches

In September 2016, Crown Melbourne conducted an Australian company search which disclosed Customer 47's business history, property holdings and liabilities.

In April 2018 and August 2020, Crown Melbourne obtained a risk intelligence, land registry, bankruptcy and Australian company search in respect of Customer 47.

Issue and revocation of a WOL in respect of Customer 47

On 20 July 2016, Crown Melbourne issued a WOL in respect of Customer 47. The WOL was lifted on 8 September 2016.

On 25 August 2017, Crown Melbourne issued a WOL in respect of Customer 47. The WOL was lifted on 23 February 2018.

On 30 April 2018, Crown Melbourne issued a WOL in respect of Customer 47. The WOL was lifted on 30 April 2019. Customer 47 continued to receive designated services from Crown Perth up until 29 January 2019.

On 19 November 2019, Crown Melbourne issued an indefinite WOL in respect of Customer 47 as a result of the SPR process.

On 15 September 2021, Crown Perth issued an NRL in respect of Customer 47.

Senior management engagement

On 30 September 2019, the Group General Manager (AML) requested the AML Melbourne team consider Customer 47 and requested documents relating to Customer 47. On 1 October 2019, the CTRM was provided with copies of a Central Credit report, Customer 47's application for a CCF, SYCO screenshots relating to Customer 47 and a number of search results relating to Customer 47.

None of these steps were proportionate to the ML/TF risks reasonably posed by Customer 47 on and from 1 March 2016.

Enhanced customer due diligence

1780. Having formed a suspicion for the purposes of s41 of the Act, Crown Melbourne gave the AUSTRAC CEO SMRs with respect to Customer 47 on:

a. 13 July 2016;

b. 31 July 2019; and

c. 16 October 2019.

Particulars

The 13 July 2016 and 31 July 2019 SMRs reported Customer 47's annual losses and the amount of cash Customer 47 was prepared to carry.

The 16 October 2019 SMR related to the $300,000 cheque presented to Crown Melbourne on 26 September 2019 that was subsequently reported as lost or stolen: see particulars at paragraph 1778. The SMR stated that Crown Melbourne inferred that Customer 47 had contacted an Australian bank to stop the cheque after presenting it to Crown.

1781. On each occasion that Crown Melbourne formed a suspicion with respect to Customer 47 for the purposes of s41 of the Act, it was required to apply its ECDD program to Customer 47.

Particulars

Rule 15.9(3) of the Rules.

1782. Crown Melbourne did not carry out appropriate risk-based ECDD measures with respect to Customer 47 on each occasion that Crown Melbourne formed a suspicion with respect to Customer 47 for the purposes of s41 of the Act.

a. There are no records of ECDD being conducted following the lodgement of any SMRs. However, on 19 November 2019, nearly a month after the 16 October 2019 SMR, Crown Melbourne decided to cease a business relationship with Customer 47 by issuing him a WOL: see paragraph 666.

b. Appropriate risk-based steps were not taken to obtain or analyse information about Customer 47's source of wealth/funds: see paragraph 667.

c. Appropriate risk-based steps were not taken to analyse and monitor Customer 47's transactions – both past and future – including to understand their economic purpose: see paragraphs 590 and 666.

d. In July 2016, August 2017, April 2018 and October 2019, Crown Melbourne senior management determined that a business relationship with Customer 47 was outside of its ML/TF risk appetite and issued Customer 47 with a WOL. However, in September 2016, February 2018 and April 2019, Crown Melbourne senior management determined that a business relationship with Customer 47 was within its risk appetite and revoked the WOL issued in respect of him. This was despite the ML/TF risks posed by Customer 47: see paragraph 668ff.

Particulars

Rules 15.9(3), 15.10(1)(c), (d), (2), (5) and (6) of the Rules.

Se particulars to paragraph 1779.

1783. By reason of the matters pleaded from paragraphs 1767 to 1782, on and from 1 March 2016, Crown Melbourne and Crown Perth:

a. did not monitor Customer 47 in relation to the provision of designated services, with a view to identifying, mitigating and managing the ML/TF risks reasonably faced; and

b. did not do so in accordance with rr 15.5 and 15.9 of the Rules.

1784. By reason of the matters pleaded at paragraph 1783, Crown Melbourne contravened s36(1) of the Act on and from 1 March 2016 to November 2019 with respect to Customer 47.

Particulars

Section 36(1) of the Act is a civil penalty provision: s36(2) of the Act.

1785. By reason of the matters pleaded at paragraph 1783, Crown Perth contravened s36(1) of the Act on and from 1 March 2016 to September 2021 with respect to Customer 47.

Particulars

Section 36(1) of the Act is a civil penalty provision: s36(2) of the Act.

Customer 48

1786. Customer 48 has been a customer of Crown Melbourne since 2 September 2010.

1787. From at least 2 September 2010, Crown Melbourne provided Customer 48 with designated services within the meaning of table 1 and table 3, s6 of the Act.

Particulars

On 2 September 2010, Crown Melbourne opened a credit facility for Customer 48, which was closed on 11 August 2016.

On 5 September 2010, Crown Melbourne opened a DAB account and safekeeping account for Customer 48, which remains open.

Between 2012 and 2019, Crown Melbourne recorded Customer 48's individual rated gaming activity to be cumulative loss of $1,721,035.

1788. From at least 1 June 2016, Customer 48 received designated services as a junket player, facilitated through three different junket operators.

Particulars

Customer 48 received designated services through the Suncity junket and two other junkets.

Between 1 June 2016 and 26 September 2017, Crown Melbourne recorded Customer 48's cumulative junket turnover to be $16,380,000 and win of $1,994,000.

Between 6 July 2019 and 31 August 2019, Crown Melbourne recorded Customer 48's cumulative junket turnover to be HKD20,065,002 and loss of HKD6,036,972.

The ML/TF risks posed by Customer 48

1789. By 1 March 2016, higher ML/TF risks were indicated by the nature and purpose of Customer 48's business relationship with Crown Melbourne, the nature of the transactions he had been conducting, together with the suspicions Crown Melbourne itself had formed with respect to Customer 48.

Particulars

Section 36(1)(a), (b) of the Act and Chapter 15 of the Rules.

Customer 48 was a junket player. He received designated services through the channel of junket programs. This channel lacked transparency: see paragraph 477.

SMRs by 1 March 2016

By 1 March 2016, Crown Melbourne had given the AUSTRAC CEO seven SMRs in relation to Customer 48 on 9 September 2010, 7 February 2012, 9 February 2012, 30 March 2012, 13 December 2013, 3 March 2014 and 10 November 2015. Each SMR reported annual wins, large cash transactions, third party transactions references to Customer 48 in open source media articles and the amount of cash Customer 48 was prepared to carry.

Law enforcement inquiry in 2012

In 2012, Crown Melbourne received a law enforcement inquiry in respect of Customer 48.

Other red flags by 1 March 2016

On 9 November 2015, a Crown Melbourne customer received a telegraphic transfer of a large sum in a foreign currency from a third party company. Crown Melbourne understood that the funds were to be transferred from the customer to Customer 48: SMR dated 10 November 2015. On 10 and 12 November 2015, Customer 48 received into his Crown Melbourne DAB account $1,000,000 and $1,114,436 respectively from the same Crown Melbourne customer.

Due diligence conducted by 1 March 2016

On 30 March 2012, Crown Melbourne was aware of an open source media article published on 26 March 2012. The article referred to another Crown Melbourne patron who was targeted by Australian law enforcement agencies in connection with a heroin trafficking and money laundering syndicate. The Crown Melbourne patron was associated with Customer 48, who was described as the richest man in a foreign country: SMR dated 30 March 2012.

On 26 November 2014, Crown Melbourne conducted a risk intelligence report which identified Customer 48 to be a foreign PEP.

On 31 March 2015, the Executive General Manager (Legal & Regulatory Services) approved Crown Melbourne continuing a business relationship with Customer 48.

By November 2015, Crown Melbourne had recorded Customer 48's business interests in SYCO.

1790. On and from 1 March 2016, Crown Melbourne rated Customer 48 to be high risk.

Particulars

On various occasions on and from 26 November 2014, Crown Melbourne rated Customer 48's risk to be high.

See paragraph 481.

1791. On and from 1 March 2016 designated services provided to Customer 48 posed higher ML/TF risks including because the provision of designated services to Customer 48 involved a combination of the following factors:

a. Customer 48 was a foreign PEP: see paragraphs 118 and 663;

b. Customer 48 was a junket player;

c. Customer 48 received high value financial (table 1, s6) and gaming services (table 3, s6) provided through multiple junket programs: see paragraph 473ff;

d. by August 2019, Crown Melbourne recorded Customer 48's junket turnover as exceeding $16,380,000 and HKD20,065,002 with a win of $1,994,000 with a loss of HKD6,036,972;

e. designated services provided to Customer 48 lacked transparency as the services were provided through the channel of junket programs: see paragraph 477(e);

f. by March 2012, Crown Melbourne were aware that Customer 48 was associated with another Crown Melbourne patron who had been targeted by Australian law enforcement agencies in connection with drug trafficking and money laundering;

g. these transactions took place against the background of:

   i. law enforcement having expressed an interest in Customer 48 in 2012;

   ii. seven SMRs being given to the AUSTRAC CEO by Crown Melbourne by 1 March 2016;

h. in 2016, Crown Melbourne received a further law enforcement inquiry in respect of Customer 48;

i. by March 2016, media articles connected Customer 48 with organised crime and instances of corruption;

j. by May 2017, media articles connected Customer 48 to the illegal laundering of timber and the transport of illegally laundered timber across national borders in contravention of local laws; and

k. by reason of the matters set out at subparagraphs a. to j. above, there were real risks that Customer 48's source of wealth and source of funds were not legitimate.

Monitoring of Customer 48's transactions

1792. At no time did Crown Melbourne appropriately monitor Customer 48's transactions on a risk-basis.

Particulars

Section 36(1)(a), (b) of the Act and Rules 15.4 to 15.8 of the Rules.

Crown Melbourne was unable to monitor the ML/TF risks posed by Customer 48's transactions appropriately because it did not make and keep appropriate records of designated services provided to junket players: see paragraph 483ff.

Crown Melbourne did not apply appropriate risk-based transaction monitoring to designated services provided to Customer 48: see paragraphs 590ff, 629 to 642 and 643 to 649.

Ongoing customer due diligence

1793. On and from 1 March 2016, on multiple occasions, the provision of designated services to Customer 48 raised red flags reflective of higher ML/TF risks.

Particulars

See paragraph 477.

In 2016, Crown Melbourne received a law enforcement inquiry in respect of Customer 48.

Between 1 June 2016 and 30 June 2016, Customer 48 was a key player on a Suncity junket program with turnover $12,880,000 and win of $1,950,000.

Between 26 August 2017 and 26 September 2017, Customer 48 was a key player in a junket program with turnover $3,500,000 and win of $44,000.

In 2017, Crown Melbourne recorded Customer 48's individual gaming activity to be win of $311,100.

Between 6 July 2019 and 7 July 2019, Customer 48 was a key player in a junket program with a turnover of HKD14,180,000 and loss of HKD151,970.

Between 1 August 2019 and 31 August 2019, Customer 48 was a key player on a Suncity junket program with an estimated turnover of HKD76,667,587.44 and loss of HKD5,885,002.

In 2019, Crown Melbourne recorded Customer 48's individual gaming activity to be loss of $6,041,970 (as at August 2019). This was a significant escalation from Customer 48's individual win in 2017.

By 31 August 2019, Customer 48 had made six losing trips to Crown Melbourne.

1794. Between at least February 2005 and March 2019 a number of widely accessible media reports were published in respect of Customer 48. These articles do not appear to have come to Crown Melbourne's attention as part of its due diligence process.

Particulars

Publicly accessible media articles from that period published:

- details of Customer 48's international business interests;
- reports that residents and monuments were relocated to give Customer 48 development rights;
- allegations that Customer 48's political connections with the Prime Minister of a foreign country were instrumental to his business success;
- allegations that Customer 48 was involved in organised crime and corruption;

- allegations that $3,700,000 had been embezzled from a casino in a foreign country owned by Customer 48's brother; and
- the arrest of Customer 48's brother in respect of drug-related charges.

1795. In June 2021 and October 2021, Crown Melbourne became aware of a number of widely accessible media reports published in respect of Customer 48 and companies associated with him.

Particulars

In June 2021, Crown Melbourne conducted open source media searches, which returned 10 articles published between 26 March 2012 and 8 October 2019.

In October 2021, Crown Melbourne conducted an open source media search in respect of a company financed by a joint venture between Customer 48 and an Australian bank.

1796. At no time did Crown Melbourne undertake appropriate risk-based customer due diligence with respect to Customer 48 with a view to identifying, mitigating and managing the ML/TF risks posed by the provision of designated services on and from 1 March 2016.

a. At no time did Crown Melbourne take appropriate steps to understand whether Customer 48's source of wealth/funds was legitimate.

b. At no time did Crown Melbourne take appropriate steps to identify or analyse the ML/TF risks of Customer 48's transactions or to consider whether they had a lawful purpose.

c. On each occasion that senior management considered whether to continue the business relationship with Customer 48, senior management failed to give adequate consideration to whether the ML/TF risks posed by Customer 49 were within Crown Melbourne's risk appetite.

Particulars

Section 36(1)(a) of the Act.

Until 2020, no due diligence steps were taken in respect of Customer 48. This was despite the fact that, by August 2019, Crown Melbourne recorded Customer 48's junket turnover as exceeding $16,380,000 and HKD20,065,002 with a win of $1,994,000 and a loss of HKD6,036,972.

The 2020 wealth report

On 8 November 2019, Crown Melbourne requested a wealth report in respect of Customer 48. The report was obtained in May 2020. The report included that Customer 48 had a high estimated net worth.

The June 2021 review

In June 2021, Crown Melbourne conducted risk intelligence, bankruptcy, visa, and Australian company searches. Crown

Melbourne also conducted open source media searches: see particulars to paragraph 1795.

The October 2021 review

In October 2021, as a result of applying the SPR process (see paragraph 1234) in respect of Customer 48, it was recommended that Customer 48 be referred to the POI Committee. Crown Melbourne took into account that an associate of Customer 48 had been investigated by a law enforcement agency for drug trafficking.

The November 2021 review

In November 2021, a KYC table games subject profile in respect of Customer 48 prepared by Crown Melbourne again recommended that Customer 48 be referred to the POI Committee.

In November 2021, Crown Melbourne conducted further company and name searches relating to Customer 48.

None of these steps were proportionate to the ML/TF risks reasonably posed by Customer 48 on and from 1 March 2016.

Enhanced customer due diligence

1797. Having formed a suspicion for the purposes of s41 of the Act, Crown Melbourne gave the AUSTRAC CEO one SMR with respect to Customer 48 on 2 September 2019.

Particulars

The SMR reported high junket losses and individual rated gaming activity.

1798. On that occasion, Crown Melbourne formed a suspicion with respect to Customer 48 for the purposes of s41 of the Act and it was required to apply its ECDD program to Customer 48.

Particulars

Rule 15.9(3) of the Rules.

1799. Crown Melbourne did not carry out appropriate risk-based ECDD measures with respect to Customer 48 following the submission of the SMR on 2 September 2019.

a. There are no records of ECDD being conducted following the lodgement of the SMR on 2 September 2019: see paragraphs 664 and 685.

b. Crown Melbourne did not have a basis to be satisfied that Customer 48's transactions had an apparent visible lawful purpose or that his source of funds was legitimate.

c. On each occasion that senior management considered whether to continue the business relationship with Customer 48, senior management failed to give adequate consideration to whether the ML/TF risks posed by Customer 49 were within Crown Melbourne's risk appetite.

Particulars

Rules 15.9(3), 15.10(1)(c), (d), (2), (5) and (6) of the Rules.

See particulars to paragraph 1796.

1800. At all times from 1 March 2016, Customer 48 was a foreign PEP.

Particulars

Section 36(1)(a)

On 26 November 2014, Crown Melbourne conducted a risk intelligence report which identified Customer 48 to be a foreign PEP.

1801. At all times from 1 March 2016, Crown Melbourne was required to apply its ECDD program to Customer 48.

Particulars

Rules 15.9(2) and 15.11 of the Rules.

See paragraphs 660, 663 and 666.

1802. Crown Melbourne did not carry out appropriate risk-based ECDD measures with respect to Customer 48 on and from 1 March 2016 given his status as a foreign PEP. In particular:

a. Crown Melbourne did not undertake a detailed analysis of Customer 48's KYC information or analyse the legitimacy of Customer 48's source of wealth/funds;

b. on occasions where senior management approved a continuing business relationship with Customer 48 as a foreign PEP, the decision did not have adequate regard to the ML/TF risks posed by Customer 48 given his status as a foreign PEP because it was part of a bulk approval process; and

c. on occasions where senior management approved continuing to provide designated services to Customer 48 as a foreign PEP, the decision did not have adequate regard to the ML/TF risks posed by Customer 48 given his status as a foreign PEP because it was part of a bulk approval process.

Particulars

Rules 15.10(2), 15.10(6), 15.11 of the Rules.

See paragraphs 1796 and 1799.

See paragraph 660, 663, 666, 667 and 668.

1803. On and from 1 March 2016, Crown Melbourne rated Customer 48 high risk.

Particulars

Crown Melbourne rated Customer 48 high risk on six occasions on and from 26 November 2014: see paragraph 1790.

1804. On each occasion that Crown Melbourne rated Customer 48 high risk, Crown Melbourne was required to apply its ECDD program to Customer 48.

Particulars

Rule 15.9(1) of the Rules.

See paragraph 661.

1805. Crown Melbourne did not carry out appropriate risk-based ECDD measures with respect to Customer 48 on each occasion that Crown Melbourne rated Customer 48 high risk.

Particulars

See paragraphs 1796, 1799 and 1802.

Other than the November 2019 high risk rating, at no time did Crown Melbourne conduct ECDD following each occasion that it rated Customer 48 high risk.

Following Crown Melbourne rating Customer 48 as high risk in November 2019, Crown Melbourne obtained a wealth report in respect of Customer 48. That wealth report identified Customer 48's net worth and significant business interests.

See paragraphs 661, 666, 667 and 668.

1806. By reason of the matters pleaded from paragraphs 1786 to 1805, on and from 1 March 2016, Crown Melbourne:

a. did not monitor Customer 48 in relation to the provision of designated services, with a view to identifying, mitigating and managing the ML/TF risks reasonably faced; and

b. did not do so in accordance with rr 15.5 and 15.9 of the Rules.

1807. By reason of the matters pleaded at paragraph 1806, Crown Melbourne contravened s36(1) of the Act on and from 1 March 2016 with respect to Customer 48.

Particulars

Section 36(1) of the Act is a civil penalty provision: s36(2) of the Act.

Customer 49

1808. Customer 49 has been a customer of Crown Melbourne since 9 June 2000.

1809. From at least March 2009, Crown Melbourne provided Customer 49 with designated services within the meaning of table 1 and table 3, s6 of the Act.

Particulars

On 27 March 2009, Crown Melbourne opened a DAB account and a safekeeping account (AUD) for Customer 49 which remains open.

On 10 September 2011, Customer 49 was made a premium program player.

Between 2012 and 2015, Crown Melbourne recorded Customer 49's individual rated gaming activity as a cumulative loss of $249,690.

Between 2016 and 2017, Crown Melbourne recorded Customer 49's individual rated gaming activity as a cumulative loss of $137,845.

1810. From at least 2018, Customer 49 received designated services at Crown Melbourne as a junket player facilitated through one junket operator.

Particulars

Customer 49 received designated services at Crown Melbourne through the Customer 4 junket program.

In 2018, Customer 49 had junket losses of at least $1,500,000.

The ML/TF risks posed by Customer 49

1811. By 1 March 2016, higher ML/TF risks were indicated by the nature and purpose of Customer 49's business relationship with Crown Melbourne, the nature of the transactions he had been conducting, together with the suspicions Crown Melbourne itself had formed with respect to Customer 49.

Particulars

Section 36(1)(a), (b) of the Act and Chapter 15 of the Rules.

SMRs

By 1 March 2016, Crown Melbourne had given the AUSTRAC CEO 9 SMRs in relation to Customer 49 – on 22 January 2009, 30 March 2009, 3 June 2009, 8 December 2009, 5 October 2010, 15 December 2010, 23 August 2011, 7 October 2011, and 29 October 2014. Each SMR reported the same patterns of suspicion relating to the annual rated gaming activity of Customer 49, large cash transactions by Customer 49, increases in Customer 49's average bet, the amounts of cash Customer 49 was prepared to carry, and Customer 49's status as a possible foreign PEP.

Collectively, the SMRs given to the AUSTRAC CEO between 22 January 2009 and 29 October 2014 reported for Customer 49 total wins of $335,820 and total losses of $613,245 over this 6-year period.

Between 2012 and 2015, Crown Melbourne recorded Customer 49's cumulative individual gaming activity to be a loss of $249,690.

Foreign PEP status

From at least 3 June 2009, Crown Melbourne was aware that Customer 49 was likely to be a foreign PEP: SMR dated 3 June 2009. On 29 October 2014, Customer 49 was first determined by Crown Melbourne to be a foreign PEP.

On 31 March 2015, the Executive General Manager (Legal and Regulatory Services) approved continuing a business relationship with a number of listed PEPs, including Customer 49.

1812. Crown Melbourne first rated Customer 49's risk as high on 26 June 2014.

Particulars

On various occasions between 22 January 2009 and 1 June 2009, Crown Melbourne rated Customer 49's risk as moderate.

On various occasions between 2 June 2009 and 25 June 2014, Crown Melbourne rated Customer 49's risk as significant.

On various occasions between 26 June 2014 and 14 December 2021, Crown Melbourne rated Customer 49's risk as high.

See paragraph 481.

1813. On and from 1 March 2016 designated services provided to Customer 49 posed higher ML/TF risks including because the provision of designated services to Customer 49 involved a combination of the following factors:

a. Customer 49 was a foreign PEP: see paragraphs 118 and 663;

b. Customer 49 was a junket player;

c. Customer 49 received high value financial (table 1, s6) and gaming services (table 3, s6) provided through a junket program: see paragraph 473ff;

d. in 2018, Customer 49's junket activity involved losses exceeding $1,500,000;

e. designated services provided to Customer 49 lacked transparency as the services were provided through the channel of junket programs: see paragraph 477(e);

f. designated services provided to Customer 49 involved large transfers from a third party; and

g. by reason of the matters set out at subparagraphs a. to f. above, there were higher ML/TF risks associated with Customer 49's source of wealth/funds.

Monitoring of Customer 49's transactions

1814. At no time did Crown Melbourne appropriately monitor Customer 49's transactions on a risk-basis.

Particulars

Section 36(1)(a), (b) of the Act and Rules 15.4 to 15.8 of the Rules.

Crown Melbourne was unable to monitor the ML/TF risks posed by Customer 49's transactions appropriately because it did not make and keep appropriate records of designated services provided to junket players: see paragraph 483ff.

Crown Melbourne did not apply appropriate risk-based transaction monitoring to designated services provided to Customer 49: see paragraphs 590ff, 629 to 642 and 643 to 649.

Ongoing customer due diligence

1815. On and from 1 March 2016, on multiple occasions, the provision of designated services to Customer 49 raised red flags reflective of higher ML/TF risks.

Particulars

See paragraphs 456ff and 477.

In 2016, Crown Melbourne recorded Customer 49's individual gaming activity to be a loss of $37,175.

On 27 September 2016, Customer 49 received a telegraphic transfer of $75,000 from a third party who was likely to be a Crown Melbourne customer: SMR dated 27 September 2016.

In 2016, Crown Melbourne recorded Customer 49's individual gaming activity to be a loss of $100,680.

In 2018, Customer 49 played on a number of junket programs and had losses of at least $1,500,000: SMR dated 10 October 2018.

On 4 January 2020, Crown Melbourne last provided Customer 49 with a designated service.

1816. At no time did Crown Melbourne undertake appropriate risk-based customer due diligence with respect to Customer 49 with a view to identifying, mitigating and managing the ML/TF risks posed by the provision of designated services on and from 1 March 2016.

a. At no time did Crown Melbourne take appropriate steps to understand whether Customer 49's source of wealth/funds was legitimate.

b. At no time did Crown Melbourne take appropriate steps to identify or analyse the ML/TF risks of Customer 49's transactions or to consider whether they had a lawful purpose.

c. At no time did Crown Melbourne give appropriate consideration to whether large and high risk transactions should be processed.

d. At no time did senior management consider whether continuing the business relationship with Customer 40 was within Crown Melbourne's ML/TF risk appetite.

Particulars

Section 36(1)(a) of the Act.

In February and August 2018, Crown Melbourne conducted risk intelligence searches.

None of these steps were reasonable or proportionate to the ML/TF risks reasonably posed by Customer 49 given his status as a foreign PEP on and from 1 March 2016.

Enhanced customer due diligence

1817. Having formed a suspicion for the purposes of s41 of the Act, Crown Melbourne gave the AUSTRAC CEO SMRs with respect to Customer 49 on:

a. 27 September 2016; and

b. 10 October 2018.

Particulars

The SMRs reported high individual losses, high junket program losses, telegraphic transfers from third parties and the amount of cash Customer 49 was prepared to carry.

1818. On each occasion that Crown Melbourne formed a suspicion with respect to Customer 49 for the purposes of s41 of the Act, it was required to apply its ECDD program to Customer 49.

Particulars

Rule 15.9(3) of the Rules.

1819. Crown Melbourne did not carry out appropriate risk-based ECDD measures with respect to Customer 49 on each occasion that Crown Melbourne formed a suspicion with respect to Customer 49 for the purposes of s41 of the Act.

a. There are no records of ECDD being conducted following the lodgement of SMRs on 27 September 2016 and 10 October 2018: see paragraphs 664 and 685.

b. Appropriate risk-based steps were not taken to obtain or analyse information about Customer 49's source of wealth/funds: see paragraph 667.

c. Appropriate risk-based steps were not taken to analyse and monitor Customer 49's transactions – both past and future – including to understand their economic purpose: see paragraphs 590 and 666.

d. At no time did senior management consider whether continuing the business relationship with Customer 40 was within Crown Melbourne's ML/TF risk appetite: see paragraph 668ff.

Particulars

Rules 15.9(3), 15.10(1)(c), (d), (2), (5) and (6) of the Rules.

See particulars to paragraph 1816.

1820. At all times from 1 March 2016, Crown Melbourne believed Customer 49 was a foreign PEP.

Particulars

Section 36(1)(a) of the Act.

See paragraph 1811.

1821. At all times from 1 March 2016, Crown Melbourne was required to apply its ECDD program to Customer 49.

Particulars

Rules 15.9(2) and 15.11 of the Rules.

See paragraphs 660, 663 and 666.

1822. Crown Melbourne did not carry out appropriate risk-based ECDD measures with respect to Customer 49 on and from 1 March 2016 given his status as a foreign PEP. In particular:

a. Crown Melbourne did not undertake a detailed analysis of Customer 49's KYC information, nor did it take reasonable measures to identify Customer 49's source of wealth/funds;

b. no steps were taken to seek and obtain senior management approval for continuing a business relationship with Customer 49 having regard to the ML/TF risks posed by the customer on and from 1 March 2016; and

c. no steps were taken to seek and obtain senior management approval for whether Crown Melbourne should continue to provide designated services to Customer 49 on and from 1 March 2016.

Particulars

Rules 15.10(2), 15.10(6), 15.11 of the Rules.

See paragraphs 1816 and 1819.

See paragraph 660, 663, 666, 667 and 668.

1823. On and from 1 March 2016, Crown Melbourne rated Customer 49 high risk.

Particulars

Crown Melbourne rated Customer 49 high risk on three occasions between 27 September 2016 and 14 December 2021: see paragraph 1812.

1824. On each occasion that Crown Melbourne rated Customer 49 high risk, Crown Melbourne was required to apply its ECDD program to Customer 49.

Particulars

Rule 15.9(1) of the Rules.

See paragraph 661.

1825. Crown Melbourne did not carry out appropriate risk-based ECDD measures with respect to Customer 49 on each occasion that Crown Melbourne rated Customer 49 high risk.

Particulars

At no time did Crown Melbourne conduct ECDD following any occasion that it rated Customer 49 high risk: see paragraphs 1816, 1819 and 1822.

See paragraphs 661, 666, 667 and 668.

1826. By reason of the matters pleaded from paragraphs 1808 to 1825, on and from 1 March 2016, Crown Melbourne:

a. did not monitor Customer 49 in relation to the provision of designated services, with a view to identifying, mitigating and managing the ML/TF risks reasonably faced; and

b. did not do so in accordance with rr 15.5 and 15.9 of the Rules.

1827. By reason of the matters pleaded at paragraph 1826, Crown Melbourne contravened s36(1) of the Act on and from 1 March 2016 with respect to Customer 49.

Particulars

Section 36(1) of the Act is a civil penalty provision: s36(2) of the Act.

Customer 50

1828. Customer 50 has been a customer of Crown Melbourne since 9 April 2004.

1829. From at least 19 April 2010, Crown Melbourne provided Customer 50 with designated services within the meaning of table 1 and table 3, s6 of the Act.

1830. From at least 19 April 2010, Customer 50 received designated services as a junket player, facilitated through 3 different junket operators.

Particulars to paragraphs 1829 and 1830

Customer 50 received designated services through the Customer 5 junket and two other junkets.

On 11 June 2019, Crown Melbourne opened a DAB account and a safekeeping account for Customer 50 under two PIDs.

From 2015, Crown Melbourne recorded that Customer 50's gaming activity on Customer 5's junkets involved turnover of $140,300,000 with losses of $1,518,020.

The ML/TF risks posed by Customer 50

1831. By 1 March 2016, higher ML/TF risks were indicated by the nature and purpose of Customer 50's business relationship with Crown Melbourne, the nature of the transactions he had been conducting, together with the suspicions Crown Melbourne itself had formed with respect to Customer 50.

Particulars

Section 36(1)(a), (b) of the Act and Chapter 15 of the Rules.

Customer 50 was a junket player. He received designated services through the channel of junket programs. This channel lacked transparency: see paragraph 477.

By 1 March 2016, Crown Melbourne had given the AUSTRAC CEO four SMRs in relation to Customer 50 on 19 April 2010, 7 January 2011, 10 January 2012 and 10 July 2013. Each SMR reported the same repeated patterns of suspicions relating to Customer 50's wins and losses under junket programs.

Collectively, the SMRs given to the AUSTRAC CEO between 19 April 2010 and 10 July 2013 reported total wins of $1,324,100 and total losses of $126,900 over this 3 year period.

1832. As at 1 March 2016, Customer 50 should have been recognised by Crown Melbourne as a high risk customer for the reasons pleaded at paragraph 1831.

Particulars

Section 36(1)(a), (b) of the Act and Chapter 15 of the Rules.

1833. At all times on and from 1 March 2016, Customer 50 should have been recognised by Crown Melbourne as a high risk customer by reason of the matters pleaded at paragraphs 1831, 1835, 1837, 1838 and 1840.

Particulars

Section 36(1)(a), (b) of the Act and Chapter 15 of the Rules.

1834. At no time was Customer 50 rated high risk by Crown Melbourne.

Particulars

On various occasions between 11 September 2017 and 4 August 2021, Crown Melbourne assessed Customer 50 as moderate risk.

See paragraph 481.

1835. On and from 1 March 2016 designated services provided to Customer 50 posed higher ML/TF risks including because the provision of designated services to Customer 50 involved a combination of the following factors:

a. Customer 50 received high value financial (table 1, s6) and gaming services (table 3, s6) provided through multiple junket programs: see paragraph 473ff;

b. Customer 50 was a junket player;

c. by no later than August 2021, Crown Melbourne recorded Customer 50's turnover on Customer 5 junket programs had exceeded $140,300,000 since July 2015;

d. designated services provided to Customer 50 lacked transparency as the services were provided through the channel of junket programs: see paragraph 477(e);

e. the table 3, s6, designated services provided to Customer 50 involved high turnover;

f. designated services provided to Customer 50 involved large transfers to third parties, including to junket operators in respect of whom Crown Melbourne had formed suspicions;

g. designated services provided to Customer 50 involved large cross-border movements of funds: see paragraph 239;

h. at various times, Customer 50 had significant parked or dormant funds in his DAB accounts: see paragraph 252; and

i. by reason of the matters set out at subparagraphs a. to h. above, there were higher ML/TF risks associated with Customer 50's source of wealth/funds.

Monitoring of Customer 50's transactions

1836. At no time did Crown Melbourne appropriately monitor Customer 50's transactions on a risk-basis.

Particulars

Section 36(1)(a), (b) of the Act and Rules 15.4 to 15.8 of the Rules.

Crown Melbourne was unable to monitor the ML/TF risks posed by Customer 50's transactions appropriately because it did not make and keep appropriate records of designated services provided to junket players: see paragraph 483ff.

Crown Melbourne did not apply appropriate risk-based transaction monitoring to designated services provided to Customer 50: see paragraphs 590ff, 629 to 642 and 643 to 649.

Ongoing customer due diligence

1837. On and from 1 March 2016, on multiple occasions, the provision of designated services to Customer 50 raised red flags reflective of higher ML/TF risks arising from Customer 50's junket activity.

Particulars

See paragraph 477.

From July 2015 to August 2021, Crown Melbourne recorded that Customer 50's turnover under junket programs operated by Customer 5 was $140,300,000 with losses of $1,518,020.

Junket activity in 2017

Between 30 August 2017 and 13 September 2017, Customer 50 attended Crown Melbourne as a key player on a junket program

operated by Customer 5 . Customer 50 lost $423,400 under the junket program.

Junket activity in 2019

Between 5 December 2018 and 12 January 2019, Customer 50 attended Crown Melbourne as a key player on a junket program operated by Customer 5. Crown Melbourne recorded that Customer 50's "estimated turnover" during the program was $20,286,900, with losses of $935,125 – representing a significant increase since the last junket program Customer 50 attended.

Following the closure of the above junket program, Crown Melbourne formed suspicions about Customer 50's losses of $935,125 under the program: SMR dated 16 January 2019.

Between 4 July 2019 to 26 July 2019, Customer 50 attended Crown Melbourne as a key player on a junket program operated by Customer 5. Crown Melbourne recorded that Customer 50's turnover during this junket was $20,591,400, with losses of $668,950.

By 30 July 2019, Crown Melbourne had formed suspicions about Customer 50's losses totalling $1,620,440 on junket programs he had attended as a key player in 2019: SMR dated 30 July 2019.

1838. On and from July 2019, the provision of designated services to Customer 50 by Crown Melbourne raised red flags reflective of higher ML/TF risks as a result of unusual transactions and patterns of transactions involving Customer 50 and other junket operators.

Particulars

See paragraph 420ff.

Unusual transactions and patterns of transactions in 2019

On 1 July 2019, Crown Melbourne received $3,000,000 sent via telegraphic transfer from Customer 50's bank account in a foreign country. The funds were deposited into Customer 50's DAB account. This amount was capable of covering his losses for the entire period of gaming with the Customer 5 junket.

On 15 July 2019 Customer 50 arranged for Crown Melbourne to withdraw $1,500,000 from his DAB account and transfer it to Customer 5's safekeeping account. Following receipt of the funds from Customer 50, on 28 August 2019, Customer 5 requested $287,868 be withdrawn from safekeeping and sent via telegraphic transfer to an overseas casino.

Between 15 July 2019 and 4 August 2021, the residual balance of $1,500,000 remained parked in Customer 50's DAB account.

Unusual transactions and patterns of transactions in 2021

On 4 August 2021, Customer 50 requested that the $1,500,000 in his DAB account be transferred to his personal bank account in a foreign country.

On 11 August 2021, Crown Melbourne remitted $1,500,000 from Customer 50's DAB account, through a Crown Patron account to an account Customer 50 held overseas.

1839. At no time did Crown Melbourne undertake appropriate risk-based customer due diligence with respect to Customer 50 with a view to identifying, mitigating and managing the ML/TF risks posed by the provision of designated services on and from 1 March 2016.

a. At no time did Crown Melbourne take appropriate steps to understand whether Customer 50's source of wealth/funds was legitimate.

b. At no time did Crown Melbourne take appropriate steps to identify or analyse the ML/TF risks of Customer 50's transactions or to consider whether they had a lawful purpose.

c. With the exception of the 4 August 2021 transfer of $1,500,000 from Customer 50's DAB account, Crown Melbourne gave no consideration at any time to whether large and high risk transactions should be processed.

d. Until September 2021, senior management failed to consider whether a business relationship with Customer 50 was within Crown Melbourne's ML/TF risk appetite. On each occasion that senior management considered whether to continue the business relationship with Customer 50, senior management failed to give adequate consideration to whether the ML/TF risks posed by Customer 50 were within Crown Melbourne's risk appetite.

Particulars

Section 36(1)(a) of the Act.

The due diligence steps taken with respect to Customer 50 included:

Due diligence conducted between 2016 and 2018

At no time between 2016 and 2018 did Crown Melbourne carry out any due diligence steps in relation to Customer 50.

Due diligence conducted in 2019

On 16 January 2019, the Group General Manager – AML reviewed Customer 50's SMR record as part of a key player review and noted that no SMR had been submitted since 2017.

On 27 August 2019, following the request by Customer 5 to transfer funds in safekeeping to an overseas casino, Crown's Group General Manager – AML queried the origin of the funds in Customer 5's safekeeping account. In response, Crown's Credit Collections Manager (VIP International) traced the funds in Customer 5's safekeeping account to a transfer from Customer 50's DAB account on 15 July 2019, following receipt of a telegraphic transfer of $3,000,000 from Customer 50's overseas bank account.

Due diligence conducted in 2021

In May 2021, Crown performed risk intelligence, media, bankruptcy and Australian company searches for Customer 50.

On 25 June 2021, 2 July 2021, 30 August 2021, and 31 August 2021, Crown Melbourne obtained a wealth report on Customer 50.

Following Customer 50's request for funds in his DAB account comprising $1,500,000 be transferred to his personal bank account, Crown employees carried out a transaction analysis of Customer 50's financial and gaming activity at Crown Melbourne, and performed database searches, including risk intelligence, media and open source searches in respect of Customer 50, his associates and companies linked to him.

Significant Player Review

By 1 September 2021, Crown identified Customer 50 through its SPR process and performed additional due diligence on him: see particulars to paragraph 1234.

On 1 September 2021, Customer 50 was given an initial risk rating of Amber and an updated net risk rating of Green.

None of these steps were proportionate to the ML/TF risks reasonably posed by Customer 50 on and from 1 March 2016.

Enhanced customer due diligence

1840. Having formed a suspicion for the purposes of s41 of the Act, Crown Melbourne gave the AUSTRAC CEO SMRs with respect to Customer 50 on:

a. 11 September 2017;

b. 16 January 2019; and

c. 30 July 2019.

Particulars

Each of these SMRs reported high losses and minimal individual rated gaming activity noting that win/losses under a junket program are not shown under a patron's individual rated gaming activity.

1841. On each occasion that Crown Melbourne formed a suspicion with respect to Customer 50 for the purposes of s41 of the Act, it was required to apply its ECDD program to Customer 50.

Particulars

Rule 15.9(3) of the Rules.

1842. Crown Melbourne did not carry out appropriate risk-based ECDD measures with respect to Customer 50 on each occasion that Crown Melbourne formed a suspicion with respect to Customer 50 for the purposes of s41 of the Act.

a. There are no records of ECDD being conducted following the lodgement of SMRs on 11 September 2017, 16 January 2019, and 30 July 2019: see paragraphs 664 and 685.

b. Appropriate risk-based steps were not taken to obtain or analyse information about Customer 50's source of wealth/funds: see paragraph 667.

c. Appropriate risk-based steps were not taken to analyse and monitor Customer 50's transactions – both past and future – including to understand their economic purpose: see paragraphs 590 and 666.

d. Until September 2021, senior management failed to consider whether a business relationship with Customer 50 was within Crown Melbourne's ML/TF risk appetite. On each occasion that senior management considered whether to continue the business relationship with Customer 50, senior management failed to give adequate consideration to whether the ML/TF risks posed by Customer 50 were within Crown Melbourne's risk appetite: see paragraph 668ff.

Particulars

Rules 15.9(3), 15.10(1)(c), (d), (2), (5) and (6) of the Rules.

See particulars to paragraph 1839.

1843. By reason of the matters pleaded from paragraphs 1828 to 1842, on and from 1 March 2016, Crown Melbourne:

a. did not monitor Customer 50 in relation to the provision of designated services, with a view to identifying, mitigating and managing the ML/TF risks reasonably faced; and

b. did not do so in accordance with rr 15.5 and 15.9 of the Rules.

1844. By reason of the matters pleaded at paragraph 1843, Crown Melbourne contravened s36(1) of the Act on and from 1 March 2016 with respect to Customer 50.

Particulars

Section 36(1) of the Act is a civil penalty provision: s36(2) of the Act

Customer 51

1845. Customer 51 was a customer of Crown Melbourne from 11 February 2012 to 2 August 2021.

1846. From at least 11 February 2012 to 2 August 2021, Crown Melbourne provided Customer 51 with designated services within the meaning of table 1 and table 3, s6 of the Act.

Particulars

On 11 February 2012, Crown Melbourne opened a DAB account and a safekeeping account for Customer 51 under two PIDs.

On 11 November 2019, Crown Melbourne issued a WOL in respect of Customer 51 and added stop codes to Customer 51's account.

1847. From at least 16 December 2012, Customer 51 received designated services as a junket operator and as a junket player, facilitated through four different junket operators at Crown Melbourne.

Particulars

On 16 December 2012, Crown Melbourne entered into a NONEGPRA with Customer 51 to operate junkets at Crown Melbourne.

Between 2013 and 2015, Customer 51 facilitated at least nine junkets at Crown Melbourne for key players, including Customer 29.

By at least February 2015, Crown Melbourne recorded Customer 51's individual gaming activity and gaming activity on junket programs run by Customer 51 as turnover of $311,664,610, with losses of $15,141,355. Commissions of $2,424,146 were payable by Crown Melbourne to Customer 51.

On 25 January 2013, Crown Melbourne approved a credit facility (AUD/HKD) for Customer 51 under the same PIDs. On 15 January 2018, Crown Melbourne closed the credit facility.

The ML/TF risks posed by Customer 51

1848. By 1 March 2016, higher ML/TF risks were indicated by the nature and purpose of Customer 51's business relationship with Crown Melbourne, the nature of the transactions he had been conducting, together with the suspicions Crown Melbourne itself had formed with respect to Customer 51.

Particulars

Section 36(1)(a), (b) of the Act and Chapter 15 of the Rules.

Customer 51 was a junket player and junket operator. He received designated services through the channel of junket programs. This channel lacked transparency: see paragraph 477.

Junket and individual gaming activity by 1 March 2016

By the end of the 2013 financial year, Crown Melbourne recorded Customer 51's individual gaming activity and gaming activity on junket programs run by Customer 51 as having turnover of $122,828,600, with losses of $3,415,175.

By the end of the 2014 financial year, Crown Melbourne recorded Customer 51's individual gaming activity and gaming activity on junket programs run by Customer 51 as having turnover of $128,458,760, with losses of $9,997,050.

By the end of the 2015 financial year, Crown Melbourne recorded Customer 51's individual gaming activity and gaming activity on junket programs run by Customer 51 as having turnover of $27,854,650, with losses of $1,196,515.

Between 2013 and 2015, Crown management regularly reapproved credit for Customer 51, up to limits of $3,000,000.

By 21 November 2015, following the closure of a junket program operated by Customer 51, Customer 51 owed Crown Melbourne a debt of $4,247,310.

SMRs by 1 March 2016

By 1 March 2016, Crown Melbourne had given the AUSTRAC CEO seven SMRs in relation to Customer 51. One SMR related to Crown Melbourne's suspicions that Customer 51 and Customer 29 were associated in some way: SMR dated 15 February 2012.

Two SMRs given to the AUSTRAC CEO related to telegraphic transfers from Customer 51's DAB account to third parties as follows.

On 14 February 2012, $3,000,000 in gaming chips were deposited into Customer 51's DAB account. The following day, $3,080,000 was withdrawn from the DAB account and sent via telegraphic transfer to a third party company based overseas. Crown Melbourne had formed suspicions that the original gaming chips in fact belonged to another Crown patron, Customer 29: SMR dated 16 February 2012.

On 5 May 2015, Crown Melbourne withdrew $3,400,000 from Customer 51's DAB account and sent it via telegraphic transfer to a third party company in Australia: SMR dated 6 March 2015.

Four SMRs related to suspicions formed by Crown Melbourne with respect to Customer 51's losses as a key player on his own junket programs. Collectively, the SMRs given to the AUSTRAC CEO between 15 January 2013 and 24 November 2015 reported total losses of $12,547,980 over a 2 year period.

Other red flags by 1 March 2016

In 2020, an independent auditor identified that Crown Melbourne received four telegraphic transfers between May 2014 and June 2014 totalling $1,706,022 into a Southbank account, for the benefit of Customer 51 from a third party foreign remittance service provider.

By 17 July 2014, Customer 51 owed a debt of $2,959,999 to Crown Melbourne, arising from an outstanding credit marker. On 18 July 2014, Crown Melbourne received two telegraphic transfers from a third party company, of $925,029.39 and $775,787.39, for the benefit of Customer 51. The Credit control team raised concerns that the funds may need to be returned to the third party company, but were advised that the company was a money changer who had changed funds for Customer 51. The funds were then applied to repay Customer 51's debt to Crown Melbourne.

Due diligence by 1 March 2016

In June 2014, the Credit control team performed Australian company and property searches for the purpose of assessing Customer 51's creditworthiness prior to reactivating Customer 51's credit facility.

In late 2015, the Credit control team conducted risk intelligence, company, bankruptcy and property searches in relation to Customer 51. Crown Melbourne requested a wealth report but a wealth report could not be prepared based on the information provided.

1849. As at 1 March 2016, Customer 51 should have been recognised by Crown Melbourne as a high risk customer for the reasons pleaded at paragraph 1848.

Particulars

Section 36(1)(a), (b) of the Act and Chapter 15 of the Rules.

1850. At all times on and from 1 March 2016, Customer 51 should have been recognised by Crown Melbourne as a high risk customer by reason of the matters pleaded at paragraphs 1848, 1852 and 1854.

Particulars

Section 36(1)(a), (b) of the Act and Chapter 15 of the Rules

1851. It was not until 4 November 2019 that Customer 51 was rated high risk by Crown Melbourne.

Particulars

On various occasions between 15 February 2012 and 24 November 2015, Crown Melbourne assessed Customer 51 as moderate risk.

On 19 October 2016, 6 February 2018 and 22 August 2019, Crown Melbourne assessed Customer 51 as significant risk.

On various occasions between 4 November 2019 and 20 January 2021, Crown Melbourne assessed Customer 51 as high risk.

See paragraph 481.

1852. On and from 1 March 2016, designated services provided to Customer 51 posed higher ML/TF risks including because the provision of designated services to Customer 51 involved a combination of the following factors:

a. Customer 51 received high value financial (table 1, s6) and gaming services (table 3, s6) provided through multiple junket programs: see paragraph 473ff;

b. Customer 51 was a junket operator who facilitated the provision of high value financial and gaming services (tables 1 and 3, s6) to key players (including foreign PEPs) on his junket programs: see paragraph 473ff;

c. Customer 51 was a junket player;

d. designated services provided to Customer 51 lacked transparency as the services were provided through the channel of junket programs: see paragraph 477(e);

e. designated services provided to Customer 51 involved large transfers to and from third parties, including to and from other junket operators, foreign remittance service providers and unknown third parties: see paragraph 456ff;

f. Customer 51 received large transfers and unusual transfers from other Australian casinos;

g. between April 2016 and August 2018, Customer 51 had significant parked or dormant funds totalling $500,000 in his safekeeping accounts: see paragraph 252;

h. these transactions took place against the background of:

i. Customer 51's individual gaming activity and gaming activity on junket programs run by Customer 51 exceeding turnover of $311,664,610 between 2012 and 2015; and

ii. seven SMRs being given to the AUSTRAC CEO by Crown Melbourne by 1 March 2016;

i. in 2016 and 2018, Customer 51 was the subject of law enforcement inquiries on two occasions;

j. in 2019, media reports named Customer 51 as:

i. allegedly associated with Customer 29;

ii. subject to civil proceedings in which freezing orders were made following allegations he had stolen casino chips from a patron at another Australian casino;

iii. subject to criminal charges in Australia for allegedly threatening to kill a man with a knife and demanding the transfer of a $10 million property; and

iv. involved in extorting a man into gambling at an Australian casino as his proxy;

k. by reason of the matters set out at subparagraphs a. to j. above, there were higher ML/TF risks associated with Customer 51's source of wealth/funds.

Monitoring of Customer 51's transactions

1853. At no time did Crown Melbourne appropriately monitor Customer 51's transactions on a risk-basis.

Particulars

Section 36(1)(a), (b) of the Act and Rules 15.4 to 15.8 of the Rules.

Crown Melbourne was unable to monitor the ML/TF risks posed by Customer 51's transactions appropriately because it did not make and keep appropriate records of designated services provided to junket players or operators: see paragraphs 483 and 485.

Crown Melbourne did not apply appropriate risk-based transaction monitoring to designated services provided to Customer 51: see paragraphs 590ff, 629 to 642 and 643 to 649.

Ongoing customer due diligence

1854. On and from 1 March 2016, the provision of designated services to Customer 51 by Crown Melbourne raised red flags reflective of higher ML/TF risks arising from:

a. unusual transactions involving third parties to repay a debt owed to Crown Melbourne;

b. law enforcement's interest in Customer 51; and

c. publicly available information in relation to Customer 51.

Particulars

Red flags in 2016

By 1 March 2016, Customer 51 owed Crown Melbourne approximately $4,247,310.

On 5 April 2016, Crown Melbourne attempted to deposit a cheque made out to Crown Limited and signed by Customer 51. By 6 April 2016, Crown Melbourne was informed that the cheque was dishonoured.

On 12 April 2016, Crown Melbourne received a telegraphic transfer of $500,000 from another Australian casino for the benefit of Customer 51, which was placed into Customer 51's safekeeping account.

The funds were parked in Customer 51's safekeeping account between 12 April 2016 and 12 August 2018.

On 19 October 2016, Crown Melbourne received an inquiry from law enforcement relating to Customer 51.

Red flags in 2018

On 6 February 2018, Crown Melbourne an inquiry from law enforcement relating to Customer 51.

On 12 August 2018, Crown Melbourne withdrew the $500,000 from Customer 51's safekeeping account. The funds were used to partially repay Customer 51's debt arising from an overdue credit marker.

Red flags in 2019

From 28 July 2019, Crown Melbourne became aware of media articles reporting that Customer 51 was allegedly associated with Customer 29 and was subject to civil proceedings in which freezing orders were made following allegations he had stolen casino chips from a patron at another Australian casino.

By 7 November 2019, Crown Melbourne became aware of media articles reporting that Customer 51 had been charged with violent offences and refused bail, and that Customer 51 was allegedly extorting a third party and using them to gamble "by proxy" at another Australian casino.

1855. At no time did Crown Melbourne undertake appropriate risk-based customer due diligence with respect to Customer 51 with a view to identifying, mitigating and managing the ML/TF risks posed by the provision of designated services on and from 1 March 2016.

a. At no time did Crown Melbourne take appropriate steps to understand whether Customer 51's source of wealth/funds was legitimate.

b. At no time did Crown Melbourne take appropriate steps to identify or analyse the ML/TF risks of Customer 51's transactions or to consider whether they had a lawful purpose.

c. At no time did Crown Melbourne give appropriate consideration to whether large and high risk transactions should be processed.

d. On each occasion prior to November 2019 that senior management considered whether to continue the business relationship with Customer 51, senior management failed to give adequate consideration to whether the ML/TF risks posed by Customer 51 were within Crown Melbourne's risk appetite.

Particulars

Section 36(1)(a) of the Act.

The due diligence steps taken with respect to Customer 51 included:

Database searches

On 15 September 2018, the Credit control team performed risk intelligence searches, Australian company and property searches in respect of Customer 51.

On 1 August 2019, the AML Manager (Crown Melbourne) performed media searches on Customer 51, using the search terms "laundering" and an organised crime syndicate.

In November 2019, Crown Melbourne obtained media articles that referred to Customer 51 being charged with a number of violent offences. The articles also reported allegations that Customer 51 was extorting a third party and using them to gamble "by proxy" at an Australian casino, from which Customer 51 had been banned.

Senior management engagement

By 26 July 2019, Crown Melbourne prepared a profile on Customer 51 for the purpose of responding to media allegations. The profile was provided to the Chief Legal Officer (Australian Resorts).

By 28 July 2019, the Group General Manager (AML) performed risk intelligence and media searches for Customer 51, which reported that a patron at another Australian casino alleged that Customer 51 stole $6,300,000 of that patron's casino winnings in May 2019, which had been paid to Customer 51 by the casino, and noted that the patron had commenced Supreme Court proceedings to freeze Customer 51's assets.

On 14 August 2019, the AML Manager (Crown Melbourne) provided the Chief Legal Officer (Australian Resorts) with the media and risk intelligence searches.

On 7 November 2019, Customer 51 was reviewed by the POI Committee. The POI Committee recommended Customer 51 be banned from Crown Melbourne.

On 11 November 2019, Crown Melbourne issued a WOL in respect of Customer 51 and added stop codes to Customer 51's account.

1856. By reason of the matters pleaded from paragraphs 1845 to 1855, on and from 1 March 2016, Crown Melbourne:

a. did not monitor Customer 51 in relation to the provision of designated services, with a view to identifying, mitigating and managing the ML/TF risks reasonably faced; and

b. did not do so in accordance with rr 15.5 and 15.9 of the Rules.

1857. By reason of the matters pleaded at paragraph 1856, Crown Melbourne contravened s36(1) of the Act on and from 1 March 2016 to 11 November 2019 with respect to Customer 51.

Particulars

Section 36(1) of the Act is a civil penalty provision: s36(2) of the Act.

Customer 52

1858. Customer 52 has been a customer of Crown Melbourne since 4 February 2011.

1859. From at least 4 February 2011, Crown Melbourne provided Customer 52 with designated services within the meaning of table 1 and table 3, s6 of the Act.

1860. From at least 4 February 2011, Customer 52 received designated services as a junket operator at Crown Melbourne.

Particulars to paragraphs 1859 and 1860

On 29 October 2010 and 2 May 2019, Crown Melbourne entered into a NONEGPRA with Customer 52 to operate junkets at Crown Melbourne.

Between 2011 and 2020, Crown Melbourne recorded that gaming activity on junkets operated by Customer 52 at Crown Melbourne involved turnover of $632,000,000.

On 11 July 2011, Crown Melbourne opened a DAB account and a safekeeping account for Customer 52 under a PID. On 17 May 2019, Crown Melbourne opened a second DAB account and safekeeping account for Customer 52 under a different PID.

On 4 February 2011, Crown Melbourne approved a credit facility (AUD/HKD) for Customer 52. On 23 November 2020, Crown Melbourne closed this credit facility.

The ML/TF risks posed by Customer 52

1861. By 1 March 2016, higher ML/TF risks were indicated by the nature and purpose of Customer 52's business relationship with Crown Melbourne, the nature of the transactions he had been conducting, together with the suspicions Crown Melbourne itself had formed with respect to Customer 52.

Particulars

Section 36(1)(a), (b) of the Act and Chapter 15 of the Rules.

Customer 52 was a junket operator. He received designated services through the channel of junket programs. This channel lacked transparency: see paragraph 477.

Crown Melbourne recorded that gaming activity on junket programs run by Customer 52 at Crown Melbourne by the end of the 2015 financial year involved turnover of approximately $12,812,000, with losses of approximately $1,283,065. Commissions of approximately $105,021 were payable by Crown Melbourne to Customer 52.

Between 2011 and 2015, Crown management approved a credit facility for Customer 52, up to limits from $500,000 to $5,000,000.

SMRs

By 1 March 2016, Crown Melbourne had given the AUSTRAC CEO three SMRs in relation to Customer 52 on 13 July 2011, 10 August 2011 and 21 September 2012.

Two of the SMRs reported Crown Melbourne's suspicions with respect to noted losses by a single key player on Customer 52's junket, totalling $577,875: SMRs dated 13 July 2011 and 21 September 2012.

The remaining SMR reported on a telegraphic transfer of $242,357 received by Crown Melbourne for the benefit of Customer 52 from a third party company based overseas: SMR dated 10 August 2011.

By 1 March 2016, Customer 52 was a foreign PEP on the basis of the positions held in political and business associations in a foreign country.

Due diligence conducted by 1 March 2016

By at least March 2015, Crown Melbourne was aware that Customer 52 and his brother guaranteed a junket operation in an overseas casino. Crown Melbourne was also aware that Customer 52 was a junket representative for another junket in a different overseas casino.

In March 2015, Crown performed risk intelligence searches and company searches in respect of Customer 52.

1862. As at 1 March 2016, Customer 52 should have been recognised by Crown Melbourne as a high risk customer because he was a PEP and for the reasons pleaded at paragraph 1861.

1863. It was not until 27 May 2021 that Customer 52 was rated high risk by Crown Melbourne.

Particulars

On various occasions between 13 July 2011 and 27 June 2019, Crown Melbourne assessed Customer 52 as moderate risk.

See paragraph 481.

1864. At all times on and from 1 March 2016. Customer 52 should have been recognised by Crown Melbourne as a high risk customer because he was a PEP and by reason of the matters pleaded at paragraphs 1861, 1865, 1866, 1867, 1868, 1870 and 1873.

Particulars

Section 36(1)(a), (b) of the Act and Chapter 15 of the Rules.

1865. On and from 1 March 2016 designated services provided to Customer 52 posed higher ML/TF risks including because the provision of designated services to Customer 52 involved a combination of the following factors:

a. Customer 52 received high value financial (table 1, s6) and gaming services (table 3, s6) provided through multiple junket programs: see paragraph 473ff;

b. Customer 52 was a junket operator who facilitated the provision of high value financial and gaming services (tables 1 and 3, s6) to key players on his junket programs: see paragraph 473ff;

c. Customer 52 was a junket operator;

d. Customer 52 was a foreign PEP: see paragraphs 118 and 663;

e. Customer 52 operated and represented other junkets at overseas casinos;

f. by no later than March 2020, Crown Melbourne recorded that turnover for Customer 52's junket had exceeded $632,000,000;

g. designated services provided to Customer 52 lacked transparency as the services were provided through the channel of junket programs: see paragraph 477(e);

h. the table 3, s6, designated services provided to Customer 52 involved escalating rates of high turnover;

i. designated services provided to Customer 52 involved large transfers to and from third parties, including to and from unknown third parties: see paragraph 456ff;

j. large values were transferred to and from Customer 52's bank accounts and his DAB account, involving the provision by Crown Melbourne of designated services within the meaning of items 31 and 32, table 1, s6 of the Act: see paragraphs 411ff and 492;

k. at various times, Customer 52 was provided with significant amounts of credit upon request, up to limits of $5,000,000: see paragraphs 280ff and 487;

l. from 24 March 2020, Customer 52 had significant parked or dormant funds of $1,270,427 in his safekeeping account: see paragraph 252;

m. these transactions took place against the background of Crown Melbourne giving the AUSTRAC CEO three SMRs relating to Customer 52 by 1 March 2016; and

n. by reason of the matters set out at subparagraphs a. to m. above, there were higher ML/TF risks associated with Customer 52's source of wealth/funds.

Monitoring of Customer 52's transactions

1866. At no time did Crown Melbourne appropriately monitor Customer 52's transactions on a risk-basis.

Particulars

Section 36(1)(a), (b) of the Act and Rules 15.4 to 15.8 of the Rules.

Crown Melbourne was unable to monitor the ML/TF risks posed by Customer 52's transactions appropriately because it did not make and keep appropriate records of designated services provided to junket players: see paragraph 483ff.

Crown Melbourne did not apply appropriate risk-based transaction monitoring to designated services provided to Customer 52: see paragraphs 590ff, 629 to 642 and 643 to 649.

Some of Customer 52's transactions were indicative of ML/TF typologies and vulnerabilities that were not detected prior to a 2021 lookback. Had appropriate risk-based transaction monitoring been

applied, these transactions could have been identified earlier: see paragraphs 686 and 687.

Transactions involving Customer 52 were identified as indicative of the ML/TF typology of parking (large balances over $50,000 parked within a DAB account or safekeeping account for over 90 days) by an independent auditor in 2021. As at 30 April 2021, Customer 52 had parked $1,270,427 in his safekeeping account for 404 days, with the last transaction occurring on the account on 24 March 2020.

Ongoing customer due diligence

1867. On and from 1 March 2016, on multiple occasions, the provision of designated services to Customer 52 by Crown Melbourne raised red flags reflective of higher ML/TF risks as a result of Customer 52's junket activity.

Particulars

See paragraph 477.

Total junket gaming activity at Crown Melbourne

By March 2020, total gaming activity on junkets run by Customer 52 at Crown Melbourne from 2011 to 2020 involved turnover of approximately $632,000,000 with losses of $1,500,000.

2016

By 10 May 2016, following the settlement of a junket program operated by Customer 52, Crown Melbourne formed suspicions with respect to high losses noted for four key players on Customer 52's junket (including Person 13), totalling $649,030: SMR dated 10 May 2016.

In FY2016, Crown Melbourne recorded Customer 52's junket turnover as $74,419,200 with losses of $140,970. Commissions of $595,353 were payable by Crown Melbourne to Customer 52.

On 10 October 2016, Customer 52 operated a junket program at Crown Melbourne. Crown Melbourne recorded the buy-in as $5,000,000 with turnover of $105,413,000, and wins of $1,445,215. Commissions of $843,304 were payable by Crown Melbourne to Customer 52.

By 21 October 2016, following the settlement of the junket program, Crown Melbourne formed suspicions with respect to high losses noted for two key players on Customer 52's junket, totalling $890,165: SMR dated 21 October 2016.

Customer 52 operated junkets at Crown Melbourne between 14 October 2016 and 15 April 2018, which involved turnover of approximately $128,000,000.

Customer 52 operated junkets at Crown Melbourne between 15 April 2018 and 1 May 2019, in respect of which Crown Melbourne recorded turnover of approximately $75,000,000.

Customer 52 operated junkets at Crown Melbourne between May 2019 and March 2020, in respect of which Crown Melbourne recorded turnover of approximately $276,000,000.

1868. On and from 1 March 2016, on multiple occasions, the provision of designated services to Customer 52 by Crown Melbourne raised red flags reflective of higher ML/TF risks as a result of unusual transactions and patterns of transactions involving Customer 52.

Particulars

See paragraph 456ff.

Between 1 March 2016 and 24 March 2020, Customer 52 engaged in a number of unusual transactions including:

- on 15 March 2016, Crown Melbourne received a telegraphic transfer of $335,731 for the benefit of Customer 52 from two third parties including Person 13;
- on 9 May 2016, Customer 52 withdrew $473,368 from his DAB account at Crown Melbourne and sent it via telegraphic transfer to a third party, Person 13;
- on 26 October 2016, Customer 52 withdrew $1,000,000 from his DAB account and sent it via telegraphic transfer to two third parties including Person 13. The following day, on 27 October 2016, Customer 52 withdrew a further $1,015,378 from his DAB account and sent it via telegraphic transfer to the same two third parties. By 4 November 2016, Crown Melbourne had formed suspicions about the transfers: SMR dated 4 November 2016;
- on 8 June 2018, Crown Melbourne received a telegraphic transfer of $1,777,740 for the benefit of Customer 52 from a third party, Person 13; and
- by at least 24 March 2020, Customer 52 transacted on his Crown Melbourne safekeeping account, and parked $1,270,427 in funds in the safekeeping account. The funds remained parked in the safekeeping account as at 30 April 2021.

1869. At no time did Crown Melbourne undertake appropriate risk-based customer due diligence with respect to Customer 52 with a view to identifying, mitigating and managing the ML/TF risks posed by the provision of designated services on and from 1 March 2016.

a. At no time did Crown Melbourne take appropriate steps to understand whether Customer 52's source of wealth or funds was legitimate.

b. At no time did Crown Melbourne take appropriate steps to identify or analyse the ML/TF risks of Customer 52's transactions or to consider whether they had a lawful purpose.

c. Senior management considered Crown Melbourne's business relationship with Customer 52 in 2017 on the basis of a junket profile prepared by the Credit control team. That decision did not adequately consider the ML/TF risks associated with Customer 52.

d. On each occasion that senior management considered whether to continue the business relationship with Customer 52, senior management failed to give adequate consideration

to whether the ML/TF risks posed by Customer 52 were within Crown Melbourne's risk appetite.

Particulars

Section 36(1)(a) of the Act.

The due diligence steps taken with respect to Customer 52 included:

Database searches

On 27 April 2016, 7 December 2016, and 10 April 2017, 2 May 2018, 25 February 2019, Crown performed risk intelligence searches relating to Customer 52 and company and open source searches for companies linked to Customer 52.

On 27 April 2016, 7 December 2016, and 10 April 2017, and early 2018, Crown performed company and open source searches on companies linked to Customer 52.

Between June 2020 and October 2020, Crown performed additional property, company, risk intelligence, and open source searches on Customer 52, his companies and his associates.

Wealth reports

On 15 March 2016, 12 April 2017, 18 April 2017, 9 April 2019, 3 May 2019, 19 February 2020, 7 July 2020, and 4 January 2021, Crown obtained wealth reports on Customer 52 which indicated that Customer 52 was involved in gambling-related enterprises overseas and held political positions.

The wealth reports dated 12 April 2017 and 19 February 2020 identified Customer 52 as a foreign PEP on the basis of positions held in political bodies and business associations in an overseas jurisdiction.

Senior management engagement

By 10 April 2017, information from the wealth reports and due diligence searches was used by the Credit control team to prepare a junket profile on Customer 52 which recommended that Crown Continue to conduct business with Customer 52.

On 20 April 2017, the VIP Operations Committee attended by a Crown Resorts director, the Chief Executive Officer (Crown Resorts), the Senior Vice President (International Business), the Group General Manager (International Business Operations) and the Chief Legal Officer (Australian Resorts), considered Customer 52's junket profile and concluded that Crown could continue conducting business with Customer 52 subject to obtaining a police check.

On 21 August 2019, and 10 June 2020, the Credit control team updated Customer 52's junket profile and recommended that Crown continue to conduct business with Customer 52.

On 30 November 2020, the Group Senior Manager AML – Customer Investigations at Crown Melbourne reviewed Customer 52's October 2020 junket profile.

None of these steps were proportionate to the ML/TF risks reasonably posed by Customer 52 on and from 1 March 2016.

By 27 May 2021, the Head of Financial Crime & Group MLRO considered Customer 52 after he was identified by Crown as a PEP on 19 February 2020 in a wealth report over 12 months prior, and determined to approve an ongoing business relationship with Customer 52, subject to policies on junket activity at Crown.

Enhanced customer due diligence

1870. Having formed a suspicion for the purpose of s41 of the Act, Crown Melbourne gave the AUSTRAC CEO SMRs with respect to Customer 52 on:

a. 10 May 2016;

b. 21 October 2016; and

c. 4 November 2016.

Particulars

The SMRs reported suspicious losses by key players under Customer 52's junkets and large transfers to third parties.

1871. On each occasion that Crown Melbourne formed a suspicion with respect to Customer 52 for the purposes of s41 of the Act, was required to apply its ECDD program to Customer 52.

Particulars

Rule 15.9(3) of the Rules.

1872. Crown Melbourne did not carry out appropriate risk-based ECDD measures with respect to Customer 52 on each occasion that Crown Melbourne formed a suspicion with respect to Customer 52 for the purposes of s41 of the Act.

a. There are no records of ECDD being conducted following the lodgement of SMRs on 10 May 2016, 21 October 2016 and 4 November 2016: see paragraphs 664 and 685.

b. Appropriate risk-based steps were not taken to obtain or analyse information about Customer 52's source of wealth/funds: see paragraph 667.

c. Appropriate risk-based steps were not taken to analyse and monitor Customer 52's transactions – both past and future – including to understand their economic purpose: see paragraphs 590 and 666.

d. On each occasion that senior management considered whether to continue the business relationship with Customer 52, senior management failed to give adequate consideration to whether the ML/TF risks posed by Customer 52 were within Crown Melbourne's risk appetite: see paragraph 668ff.

Particulars

Rules 15.9(3), 15.10(1)(c), (d), (2), (5) and (6) of the Rules.

See paragraph 1869.

1873. At all times from 1 March 2016, Customer 52 was a foreign PEP for the reasons pleaded at paragraphs 1861 and 1862.

Particulars

Section 36(1)(a)

By 1 March 2016, Customer 52 was a foreign PEP on the basis of the positions held in political and business associations in a foreign country.

1874. At all times from 1 March 2016, Crown Melbourne was required to apply its ECDD program to Customer 52.

Particulars

Rules 15.9(2) and 15.11 of the Rules.

See paragraphs 660, 663 and 666.

1875. Crown Melbourne did not carry out appropriate risk-based ECDD measures with respect to Customer 52 on and from 1 March 2016 given his status as a foreign PEP. In particular:

a. Crown Melbourne did not undertake a detailed analysis of Customer 52's KYC information or analyse the legitimacy of Customer 52's source of wealth/funds;

b. senior management approval for Crown Melbourne to continue a business relationship with Customer 52 did not give adequate consideration to the ML/TF risks posed by the customer; and

c. senior management approval for Crown Melbourne to continue to provide designated services to Customer 52 did not give adequate consideration to the ML/TF risks posed by the customer.

Particulars

Rules 15.10(2), 15.10(6), 15.11 of the Rules.

Crown Melbourne did not identify Customer 52 as a PEP until 19 February 2020 and failed to rate Customer 52 as high risk at that time.

See paragraphs 1869 and 1872.

See paragraphs 660, 663, 666, 667 and 668.

1876. On and from 27 May 2021, Crown Melbourne rated Customer 52 as high risk.

Particulars

Crown Melbourne rated Customer 52's risk to be high on 27 May 2021: see paragraph 1863.

1877. On each occasion that Crown Melbourne rated Customer 52 high risk, Crown Melbourne was required to apply its ECDD program to Customer 52.

Particulars

Rule 15.9(1) of the Rules.

See paragraph 661.

1878. Crown Melbourne did not carry out appropriate risk-based ECDD measures with respect to Customer 52 on each occasion that Crown Melbourne rated Customer 52 high risk.

Particulars

At no time did Crown Melbourne conduct ECDD following each occasion that it rated Customer 52 as high risk.

See paragraphs 661, 666, 667 and 668.

1879. By reason of the matters pleaded from paragraphs 1858 to 1878, on and from 1 March 2016, Crown Melbourne:

a. did not monitor Customer 52 in relation to the provision of designated services, with a view to identifying, mitigating and managing the ML/TF risks reasonably faced; and

b. did not do so in accordance with rr 15.5 and 15.9 of the Rules.

1880. By reason of the matters pleaded at paragraph 1879, Crown Melbourne contravened s36(1) of the Act on and from 1 March 2016 with respect to Customer 52.

Particulars

Section 36(1) of the Act is a civil penalty provision: s36(2) of the Act.

DOMESTIC CUSTOMERS

Customer 53

1881. Customer 53 has been a customer of Crown Melbourne since October 2017.

1882. From at least October 2017, Crown Melbourne provided Customer 53 with designated services within the meaning of table 1 and table 3, s6 of the Act.

Particulars

On 22 October 2017, Crown Melbourne opened a DAB account and a safekeeping account for Customer 53. On 24 October 2017, Crown Melbourne opened a further DAB account and safekeeping account for Customer 53 under a second PID.

Between 2017 and 5 January 2022, Crown Melbourne recorded Customer 53's cumulative buy-in to be $8,205,225, cumulative turnover to be $42,819,323 and cumulative loss to be $731,817.

1883. Customer 53 has been a customer of Crown Perth since at least March 2019.

1884. From at least March 2019 to at least April 2019, Crown Perth provided Customer 53 with designated services within the meaning of table 1 and table 3, s6 of the Act.

Particulars

On 29 March 2019, Crown Perth opened a DAB account and a safekeeping account for Customer 53.

Between 28 March 2019 and 1 April 2019, Customer 53 participated in a VIP interstate trip with a turnover of $264,000 and a win of $24,000.

The ML/TF risks posed by Customer 53

1885. On and from November 2017, Customer 53 should have been recognised by Crown Melbourne as a high risk customer for the reasons pleaded at paragraphs 1887, 1888, 1889 and 1891.

Particulars

Section 36(1)(a), (b) of the Act and Chapter 15 of the Rules.

1886. At no time was Customer 53 rated high risk by Crown Melbourne.

Particulars

On various occasions between 17 November 2017 and 19 May 2021, Crown Melbourne assessed Customer 53's risk to be moderate.

This was despite that, in November 2017, Crown Melbourne identified that Customer 53 had been withdrawing funds from his account and obtaining multiple TITO tickets, often in sub-threshold quantities, and then depositing the TITO tickets back into his account after play.

See paragraph 120.

1887. On and from October 2017 designated services provided to Customer 53 posed higher ML/TF risks including because the provision of designated services to Customer 53 involved a combination of the following factors:

a. Customer 53 received high value financial (table 1, s6) and gaming services (table 3, s6);

b. by no later than 5 January 2022, Customer 53's turnover at Crown Melbourne had exceeded $42,000,000 with a buy-in of $8,205,225 with a loss of $731,817. By no later than April 2019, Customer 53's turnover at Crown Perth had exceeded $260,000 with a win of $24,000;

c. large values were transferred to and from Customer 53's bank accounts and his DAB account, involving the provision by Crown Melbourne of designated services within the meaning of items 31 and 32, table 1, s6 of the Act: see paragraph 411ff;

d. Customer 53 engaged in other transactions indicative of ML/TF typologies and vulnerabilities, including structuring: see paragraph 24;

e. Customer 53 engaged in repeated large and suspicious transactions involving cash value instruments and in particular ticket in ticket out instruments. Between March 2019 and February 2021, Customer 53 deposited $514,585 in cash chips and withdrew $638,000 in CPVs;

f. Customer 53 engaged in gaming activity at Crown Perth that was not commensurate with the funds he had exchanged for CPVs;

g. between 2017 and November 2020, Customer 53's turnover was close to $40,000,000. In November 2020, Customer 53 completed a source of wealth declaration which

identified his annual income to be between $0 and $250,000 and his profession to be a retired casual teacher; and

h. by reason of the matters set out at subparagraphs a. to g. above, there were higher ML/TF risks associated with Customer 53's source of wealth/funds.

Monitoring of Customer 53's transactions

1888. At no time did Crown Melbourne or Crown Perth appropriately monitor Customer 53's transactions on a risk-basis.

Particulars

Section 36(1)(a), (b) of the Act and Rules 15.4 to 15.8 of the Rules.

Crown Melbourne and Crown Perth did not apply appropriate risk-based transaction monitoring to designated services provided to Customer 53: see paragraphs 590ff and 629 to 642.

Customer 53's transactions involved repeated transactions indicative of ML/TF typologies and vulnerabilities that were not detected prior to a 2021 lookback. Had appropriate risk-based transaction monitoring been applied, these transactions could have been identified earlier: see paragraphs 686 and 687.

On 5 January 2022, as result of a lookback in respect of Customer 53, Crown Melbourne identified that the spike in buy-in and turnover in 2019 and 2020 appeared inconsistent with Customer 53's reported wealth: see paragraph 1890. Crown Melbourne noted that it was possible that those figures were inflated as a result of Customer 53's pattern of depositing TITOs at the close of each gaming session and exchanging them for gaming chips before depositing them into his DAB account. Crown Melbourne recognised that Customer 53 had a pattern of behaviour of intentionally redeeming TITOs below the reporting threshold requirement since 2017: SMR dated 5 January 2022.

Repeated patterns of unusual TITO activity

Transactions involving Customer 53 were identified as unusual by an independent auditor in 2021. The report found that Customer 53's DAB account exhibited a repeated pattern of unusual TITO activity, with multiple TITO deposits (typically under $10,000) combined with a single large withdrawal that closely reflected the value of the combined deposits. The report noted that the timestamp associated with all these transactions occurred at the same time or differed only by one minute which suggested that the transactions were being processed at the same time.

The report identified two example transactions. On 3 February 2019, Customer 53 engaged in 14 transactions over a two-minute period, comprising 13 deposits (all under $10,000 and totalling $106,939), and then one withdrawal for $115,000. On 18 April 2019 six TITO deposits totalling $58,194, and a single TITO withdrawal for $60,000, were all processed at the same time for Customer 53's DAB account.

Transactions indicative of ML/TF typologies – CVIs Chip Purchase

Transactions at Crown Melbourne involving Customer 53 were identified as indicative of the ML/TF typology of CVIs chip purchases by an independent auditor in 2021. Between 2 March 2019 and 7 February 2021, those transactions involved $514,585 in deposits of cash chips and $638,000 in withdrawals of CPVs:

- on 2 March 2019, Customer 53 deposited $75,085 in cash chips and withdrew $105,000 as a CPV;
- on 22 March 2019, Customer 53 deposited $90,000 in cash chips and withdrew $123,000 as a CPV;
- on 30 November 2019, Customer 53 deposited $56,000 in cash chips and withdrew $60,000 in a CPV;
- on 1 December 2019, Customer 53 deposited $60,000 in cash chips and withdrew $78,000 in a CPV followed by a further deposit of $60,000 in cash chips and withdrew a further $65,000 in a CPV;
- on 16 January 2020, Customer 53 deposited $60,000 in cash chips and withdrew $78,000 in a CPV;
- on 22 February 2020, Customer 53 deposited $58,450 in cash chips and withdrew $69,000 in a CPV; and
- on 6 February 2021, Customer 53 deposited $7,050 in cash chips and withdrew $60,000 in a CPV followed by a further deposit of $48,000 in cash chips on the next day.

Transactions indicative of ML/TF typologies – value of chips redeemed exceeded buy-in value

On four occasions between 5 March 2018 and 1 April 2019, the total value of chips redeemed by Customer 53 exceeded the total buy-in value within a 48-hour period without sufficient gaming winnings to explain the additional chips redeemed. The transactions involved a total deposit of $178,000 and a total withdrawal of $895,395:

- between 5 March 2018 and 7 March 2018, Customer 53 made total deposits of $20,000 and total withdrawals of $76,000 at Crown Melbourne;
- on 10 January 2019, Customer 53 made total deposits of $20,000 and total withdrawals of $183,000 at Crown Melbourne;
- between 7 March 2019 and 8 March 2019, Customer 53 made total deposits of $30,000 and total withdrawals of $300,400 at Crown Melbourne; and
- between 30 March 2019 and 1 April 2019, Customer 53 made total deposits of $108,000 and total withdrawals of $335,995 at Crown Perth,

Transactions indicative of ML/TF typologies – structuring

Transactions involving Customer 53 were identified as indicative of the ML/TF typology of structuring by an independent auditor in 2021.

Ongoing customer due diligence

1889. On and from October 2017, on multiple occasions, the provision of designated services to Customer 53 by Crown Melbourne and Crown Perth raised red flags reflective of higher ML/TF risks.

Particulars

See paragraph 420ff, 428, 433 and 435.

Unusual transactions and patterns of transactions in 2017

In 2017, Customer 53 had a buy-in of $152,800, a turnover of $1,515,171 with a loss of $2,704 at Crown Melbourne.

On 16 November 2017, Customer 53 presented six TITO tickets, each with value $5,000, and requested cash for them. Crown Melbourne identified that Customer 53 had been withdrawing funds from his account and obtaining multiple TITO tickets, often in sub-threshold quantities, and then depositing the TITO tickets back into his account after play: SMR dated 16 November 2017.

Unusual transactions and patterns of transactions in 2018

In 2018, Customer 53 had a buy-in of $584,600, a turnover of $16,715,117 with a loss of $56,098 at Crown Melbourne.

On 9 November 2018, Customer 53 transferred $138,000 to his DAB account.

On 11 November 2018, Customer 53 was paid out to his Crown Melbourne DAB account cancel credits for eight table games in various amounts ranging between $10,000 and $20,000 totalling $117,101.

Unusual transactions and patterns of transactions in 2019

In 2019, Customer 53 had a buy-in of $5,963,400, a turnover of $19,630,767 with a loss of $409,393 at Crown Melbourne.

Between 28 March 2019 and 1 April 2019, Customer 53 travelled to Crown Perth as part of a VIP interstate group. In that period, Customer 53 made three telegraphic transfers from his personal account to his Crown Perth DAB account through a Riverbank account totalling $314,000. Customer 53 exchanged the funds for CPVs and then exchanged the vouchers for chips. Customer 53 had a turnover of $264,000 with a win of $24,000. However, Customer 53's play was not commensurate with the funds that he exchanged for CPVs. Crown Perth indicated that it was possible that Customer 53 had given some chips to other patrons to play with, however could not confirm that suspicion: SMR dated 3 April 2019.

On 1 April 2019, Customer 53 withdrew $335,955 from his Crown Perth DAB account and sent it by telegraphic transfer to his personal account.

On 4 April 2019, Customer 53 was paid out to his Crown Melbourne DAB account cancel credits for five table games in various amounts ranging between $11,500 and $12,440 totalling $57,991.

On 29 April 2019, Customer 53 made an account deposit of $17,000 at Crown Melbourne.

Unusual transactions and patterns of transactions in 2020

In 2020, Customer 53 had a buy-in of $1,169,425, a turnover of $2,844,910 with a loss of $160,337 at Crown Melbourne.

Unusual transactions and patterns of transactions in 2021

In 2021, Customer 53 had a buy-in of $335,000, a turnover of $2,108,871 with a loss of $104,346 at Crown Melbourne.

Unusual transactions and patterns of transactions in 2022

By 5 January 2022, Customer 53 had a turnover of $4,487 with a win of $1,061 at Crown Melbourne.

1890. At no time did Crown Melbourne or Crown Perth undertake appropriate risk-based customer due diligence with respect to Customer 53 with a view to identifying, mitigating and managing the ML/TF risks posed by the provision of designated services on and from October 2017.

a. Until November 2020, Crown Melbourne did not take appropriate steps to understand Customer 53's source of wealth/funds. Until January 2022, Crown Melbourne did not take appropriate steps to understand whether that source of wealth/funds was legitimate.

b. Until January 2022, Crown Melbourne did not take appropriate steps to identify or analyse the ML/TF risks of Customer 53's transactions or to consider whether they had a lawful purpose.

c. At no time did Crown Melbourne give appropriate consideration to whether large and high risk transactions should be processed.

d. Senior management failed to consider whether a business relationship with Customer 53 was within Crown Melbourne's ML/TF risk appetite.

e. On each occasion that senior management considered whether to continue the business relationship with Customer 53, senior management failed to give adequate consideration to whether the ML/TF risks posed by Customer 53 were within Crown Melbourne's risk appetite.

Particulars

Section 36(1)(a) of the Act.

The due diligence steps taken by with respect to Customer 53 included:

On 17 September 2018, the Group General Manager (AML) emailed the VIP International teams requesting any due diligence conducted in respect of Customer 53. The VIP International team responded that

no due diligence had been conducted in respect of Customer 53 to date. This was despite the SMR given to the AUSTRAC CEO nearly a year earlier and Customer 53's significant turnover in 2017. No due diligence was conducted as a result of this request.

Until August 2019, despite Customer 53's turnover exceeding $20,000,000, Crown Melbourne took no steps to determine Customer 53's source of wealth/funds.

On 8 August 2019, the AML Manager (Crown Melbourne) requested that the VIP International team obtain a wealth report in respect of Customer 53. A report was requested but not provided due to insufficient information.

In August 2020, Crown Melbourne conducted open source media searches, risk intelligence searches, land registry searches and Australian company searches in respect of Customer 53.

In October 2020, Crown Melbourne produced a KYC profile in respect of Customer 53 which stated that Customer 53 was a high school tutor and sports coach.

Until November 2020, despite Customer 53's turnover approaching $40,000,000, Crown Melbourne had no verified information in respect of Customer 53's source of wealth/funds.

On 20 November 2020, Customer 53 completed a source of wealth declaration which identified his annual income to be between $0 and $250,000 and his profession to be a retired casual teacher. Customer 53 identified additional sources of income as an inheritance and share portfolio with a value not commensurate with his gaming activity. In 2022, Crown Melbourne identified that this additional source of income would substantiate Customer 53's turnover and losses, but that his 2019 buy-in did not appear consistent with his reported income: SMR dated 5 January 2022.

On 10 May 2021, the CTRM emailed the Gaming Integrity Manager (Gaming Machines) asking whether due diligence had ever been conducted in respect of Customer 53 and whether he was comfortable with Customer 53's gaming activity. The CTRM noted that Customer 53 had high turnover and significant losses over time and that Customer 53 ordinarily took one TITO from his DAB account and deposited multiple TITOs during play.

On 19 May 2021, the Gaming Integrity Manger responded saying that Customer 53 was well known from a payout perspective. The Gaming Integrity Manager said that Customer 53 played up to eight units at any given time on the circular pit therefore making it nearly impossible for Crown Melbourne to verify his ticket redemption against his rated play. On the same day, the Casino Manager (Table Games) said that Customer 53 often played on multiple terminals, predominantly in the morning and early afternoon to avoid other players.

In October 2021, Crown Melbourne conducted Australian company, bankruptcy, open source media, risk intelligence, land registry and property valuation searches in respect of Customer 53 and his alias, which returned no relevant results. Despite Crown Melbourne being aware of Customer 53's alias from at least September 2018, these were the first due diligence searches which included his alias as a search term.

In November 2021, Crown Melbourne applied the SPR process to Customer 53 and determined his risk level to be green (-0.5). The SPR records identify that Crown Melbourne had not identified Customer 53's occupation and also incorrectly indicate that Customer 53 had not been subject to any SMRs in the previous five years.

None of these steps were proportionate to the ML/TF risks reasonably posed by Customer 53 on and from October 2017.

On 5 January 2022, Crown Melbourne conducted a lookback in respect of Customer 53: see particulars to paragraph 1888.

Enhanced customer due diligence

1891. Having formed a suspicion for the purposes of s41 of the Act, Crown Melbourne gave the AUSTRAC CEO SMRs with respect to Customer 53 on:

a. 16 November 2017;

b. 18 April 2019; and

c. 5 January 2022.

Particulars

The 16 November 2017 and 18 April 2019 SMRs related to Customer 53's suspicious TITO transactions, Customer 53's annual losses and the amount of cash Customer 53 was prepared to carry.

The 5 January 2022 SMR comprised a lookback of Customer 53's activity at Crown Melbourne.

1892. Having formed a suspicion for the purposes of s41 of the Act, Crown Perth gave the AUSTRAC CEO SMRs with respect to Customer 53 on 3 April 2019.

Particulars

The SMR reported that Customer 53's recorded play during the March – April 2019 VIP program was not commensurate with his front money or the CPVs that he purchased: see paragraph 1887 and the particulars to paragraph 1889.

1893. On each occasion that Crown Melbourne or Crown Perth formed a suspicion with respect to Customer 53 for the purposes of s41 of the Act, it was required to apply its ECDD program to Customer 53.

Particulars

Rule 15.9(3) of the Rules.

1894. Crown Melbourne and Crown Perth did not carry out appropriate risk-based ECDD measures with respect to Customer 53 on each occasion that Crown Melbourne formed a suspicion with respect to Customer 53 for the purposes of s41 of the Act.

a. There are no records of ECDD being conducted by Crown Melbourne or Crown Perth following the lodgement of any SMR: see paragraphs 664 and 685.

b. Until January 2022, appropriate risk-based steps were not taken to obtain or analyse information about Customer 53's source of wealth/funds: see paragraph 667.

c. Until January 2022, appropriate risk-based steps were not taken to analyse and monitor Customer 53's transactions – both past and future – including to understand their economic purpose: see paragraphs 590 and 666.

d. On each occasion that senior management considered whether to continue the business relationship with Customer 53, senior management failed to give adequate consideration to whether the ML/TF risks posed by Customer 53 were within Crown Melbourne's risk appetite: see paragraph 668ff.

Particulars

Rules 15.9(3), 15.10(1)(c), (d), (2), (5) and (6) of the Rules.

See particulars to paragraph 1890.

1895. By reason of the matters pleaded from paragraphs 1881 to 1894, on and from October 2017, Crown Melbourne:

a. did not monitor Customer 53 in relation to the provision of designated services, with a view to identifying, mitigating and managing the ML/TF risks reasonably faced; and

b. did not do so in accordance with rr 15.5 and 15.9 of the Rules.

1896. By reason of the matters pleaded at paragraph 1895, Crown Melbourne contravened s36(1) of the Act on and from October 2017 with respect to Customer 53.

Particulars

Section 36(1) of the Act is a civil penalty provision: s36(2) of the Act.

1897. By reason of the matters pleaded from paragraphs 1881 to 1894, on and from 3 April 2019, Crown Perth did not:

a. did not monitor Customer 53 in relation to the provision of designated services, with a view to identifying, mitigating and managing the ML/TF risks reasonably faced; and

b. did not do so in accordance with rr 15.5 and 15.9 of the Rules.

1898. By reason of the matters pleaded at paragraph 1897, Crown Perth contravened s36(1) of the Act on and from April 2019 with respect to Customer 53.

Particulars

Section 36(1) of the Act is a civil penalty provision: s36(2) of the Act.

Customer 54

1899. Customer 54 has been a customer of Crown Melbourne since 4 April 2018 until May 2021.

1900. From at least 30 August 2018 to May 2021, Crown Melbourne provided Customer 54 with designated services within the meaning of table 1 and table 3, s6 of the Act.

Particulars

Customer 54 registered at Crown Melbourne as a domestic player with a Tasmanian address.

On 2 May 2019, Crown Melbourne opened a DAB account and a safekeeping account for Customer 54.

Customer 54 played on a number of incentive-based programs for domestic players. Customer 54 frequently stayed at the Crown Towers or Crown Promenade properties when visiting Crown Melbourne.

Between 2018 and 2021, Crown Melbourne recorded Customer 54's individual rated gaming activity to be a cumulative turnover of $52,000,000 with a loss of $1,062,750.

Customer 54 had a total of $1,800,000 in cash deposits into his DAB account and a further $1,800,000 on table or buy-in facility chip purchases during his time playing at Crown Melbourne.

On 13 May 2021, Crown Melbourne issued a WOL in respect of Customer 54.

1901. On 1 December 2020, Crown Melbourne first rated Customer 54 as high risk.

Particulars

On various occasions between 11 December 2018 and 30 November 2020, Crown Melbourne rated Customer 54 as moderate risk.

On various occasions between 1 December 2020 and 11 May 2021, Crown Melbourne rated Customer 54 as high risk.

See paragraph 120.

The ML/TF risks posed by Customer 54

1902. On and from August 2018, designated services provided to Customer 54 posed higher ML/TF risks including because the provision of designated services to Customer 54 involved a combination of the following factors:

a. Customer 54 received high value financial (table 1, s6) and gaming services (table 3, s6);

b. by 2022, Crown Melbourne recorded Customer 54's individual rated gaming activity to be a cumulative turnover of $52,000,000 with a loss of $1,062,750. On and from 2019, Customer 54's turnover escalated significantly;

c. Customer 54 carried and transacted using large amounts of cash and cash that appeared suspicious, including in $50 notes bundled in rubber bands: see paragraphs 450, 451 and 452;

d. Customer 54 was associated with another customer who had been issued a WOL due to using counterfeit notes, and who was a person of interest in a money laundering investigation. Customer 54 signed this person into the Mahogany Room on a number of occasions;

e. Customer 54 engaged in other transactions indicative of ML/TF typologies and vulnerabilities, including repeated structuring: see paragraph 24;

f. by November 2020, Crown Melbourne were aware that Customer 54's declared income and business interests did not explain his very high turnover and losses;

g. in March 2021, Customer 54 refused to provide further information regarding his source of wealth;

h. Customer 54 provided inconsistent and fraudulent details regarding his address;

i. Customer 54 provided a fraudulent utility bill as evidence of his address; and

j. by reason of the matters set out at subparagraphs a. to i. above, there were real risks that Customer 54's source of wealth and source of funds were not legitimate.

Monitoring of Customer 54's transactions

1903. At no time did Crown Melbourne appropriately monitor Customer 54's transactions on a risk-basis.

Particulars

Section 36(1)(a), (b) of the Act and Rules 15.4 to 15.8 of the Rules.

Crown Melbourne did not apply appropriate risk-based transaction monitoring to designated services provided to Customer 54: see paragraphs 590ff and 629 to 642.

Customer 54's transactions involved repeated transactions indicative of ML/TF typologies and vulnerabilities that were not detected prior to a 2021 lookback. Had appropriate risk-based transaction monitoring been applied, these transactions could have been identified earlier: see paragraphs 686 and 687.

Transactions indicative of the ML/TF typology of structuring

Transactions involving Customer 54 were identified as indicative of the ML/TF typology of structuring by an independent auditor in 2021.

Between 7 June 2019 and 29 July 2021, 31 transactions totalling $139,300 were identified:

- between 7 and 8 June 2019, two transactions totalling $10,800;
- between 16 and 18 June 2019, three transactions totalling $14,500;
- between 23 and 27 June 2019, six transactions totalling $19,700;
- between 30 June 2019 and 2 July 2019, five transactions totalling $26,400;
- between 14 and 15 July 2019, two transactions totalling $16,500;

- between 18 July and 21 July 2019, four transactions totalling $16,000;
- between 24 and 25 July 2019, three transactions totalling $12,400;
- between 29 July and 1 August 2019, two transactions totalling $15,000;
- between 12 and 13 January 2020, two transactions totalling $11,600; and
- between 19 and 29 July 2021, two transactions totalling $8,000.

Crown Melbourne's 2022 lookback

In January 2022, Crown Melbourne conducted a lookback in respect of Customer 54: SMR dated 31 January 2022. The lookback identified that Customer 54 had been issued a WOL due to doubts in respect of the plausibility of his source of funds/wealth, and unusual and large cash transactions, and Customer 54's provision to Crown Melbourne of a fraudulent address.

The lookback reported that:

- Customer 54 was not listed as the proprietor of either domicile he had identified to Crown Melbourne;
- Customer 54 had reported to Crown Melbourne that he had net worth that was not commensurate with his gaming activity;
- Customer 54 was involved in the importation of products and refused to provide supporting information to substantiate his business interests;
- there was strong evidence that Customer 54 had falsified domicile status to access domestic incentive programs; and
- Customer 54 was a cash player who requested gaming cheques which heightened the ML risk of attempts to legitimise cash as casino winnings.

Ongoing customer due diligence

1904. On and from 2018, on multiple occasions, the provision of designated services to Customer 54 by Crown Melbourne raised red flags reflective of higher ML/TF risks.

Particulars

See paragraph 450 and 451.

During the following times, designated services provided to Customer 54 involved complex, unusual large transactions and unusual patterns of transactions which had no apparent economic or visible lawful purpose.

Large and unusual transactions and patterns of transactions in 2018

In 2018, Crown Melbourne recorded Customer 54's individual rated gaming activity to be a loss of $140,300 with an average bet of $422.

Large and unusual transactions and patterns of transactions in 2019

In 2019, Crown Melbourne recorded Customer 54's individual rated gaming activity to be a loss of $335,885 with an average bet of $1,039.

On 2 July 2019, Customer 54 deposited $19,000 into his DAB account and withdrew $18,650 in cash on the same day.

On 3 July 2019, Customer 54 made two cash withdrawals of $15,500 and $10,000 within 15 minutes of each other.

Large and unusual transactions and patterns of transactions in 2020

In 2020, Crown Melbourne recorded Customer 54's individual rated gaming activity to be a turnover of $10,491,759, loss of $480,630 with an average bet of $1,546. Customer 54's turnover increased significantly: SMR dated 15 January 2021.

In January 2020, Customer 54 was warned about depositing and withdrawing cash without gaming activity.

In February 2020, Customer 54 had a buy-in of $602,700, average bet of $1,365.64, loss of $16,990 and turnover of $1,310,883.68.

In March 2020, Customer 54 had a buy-in of $900,400, average bet of $1,551.10, loss of $93,725 and turnover of $2,898,925.

Customer 54 had no rated play between March 2020 and November 2020 due to COVID-19 lockdowns in Melbourne. Crown Melbourne re-opened (with strict patron capacity limits, including time limits) on 25 November 2020.

In November 2020, Customer 54 had a buy-in of $65,000, average bet of $2,007.37, win of $20,200 and turnover of $132,323.33.

In December 2020, Customer 54 had a buy-in of $978,365, average bet of $2,000.75, loss of $351,500 and turnover of $6,149,627.53.

On 6 December 2020, Customer 54 requested a cash $10,000 buy-in. When he was asked for his identification documents during the buy-in, Customer 54 asked for $1,000 back from the $10,000: SMR dated 15 January 2021.

On 7 December 2020, Customer 54 presented $35,000 in $50 notes to buy-in.

On 15 December 2020, Customer 54 presented with $40,000 in $50 notes that were bundled in lots of $5,000 in elastic bands. He asked to exchange the money for commission based chips.

Large and unusual transactions and patterns of transactions in 2021

In February 2021, Customer 54 attended Crown Melbourne on a domestic program and funded his play with significant cash buy-ins.

In 2021, Crown Melbourne recorded Customer 54's individual rated gaming activity to be a loss of $105,935.

1905. On and from August 2018, on multiple occasions, the provision of designated services to Customer 54 raised red flags reflective of higher ML/TF risks as a result of Customer 54's association with a person of interest to law enforcement in connection with money laundering.

Particulars

Customer 54 was associated with Person 53, a person of interest to law enforcement in relation to a money laundering investigation in 2017. Person 53 was a former customer of Crown Melbourne. Crown Melbourne had issued a WOL in respect of Person 53 on 24 March 2019 for counterfeit currency.

Between September and November 2018, Customer 54 signed Person 53 into the Mahogany Room as his guest on 14 occasions.

1906. At no time did Crown Melbourne undertake appropriate risk-based customer due diligence with respect to Customer 54 with a view to identifying, mitigating and managing the ML/TF risks posed by the provision of designated services on and from 1 March 2016.

a. At no time did Crown Melbourne take appropriate steps to understand whether Customer 54's source of wealth/funds was legitimate.

b. At no time did Crown Melbourne take appropriate steps to identify or analyse the ML/TF risks of Customer 54's transactions or to consider whether they had a lawful purpose.

c. At no time did Crown Melbourne give appropriate consideration to whether large and high risk transactions should be processed.

d. On each occasion prior to May 2021 that senior management considered whether to continue the business relationship with Customer 54, senior management failed to give adequate consideration to whether the ML/TF risks posed by Customer 54 were within Crown Melbourne's risk appetite.

e. On 30 November 2020, the Gaming Integrity Manager raised concerns regarding the risks presented by Customer 54 specifically and also Crown Melbourne's approach to evaluating customer risk generally.

f. It was not until late February 2021 that any steps were taken to properly consider and analyse the ML risks presented by Customer 54.

g. It was not until May 2021 that Crown Melbourne issued a WOL in respect of Customer 54.

Particulars

Section 36(1)(a) of the Act.

The due diligence steps taken with respect to Customer 54 included:

Until November 2020, no due diligence steps were taken in respect of Customer 54.

Senior management engagement – the November 2020 review

On 28 November 2020, Customer 54 attended Crown Melbourne with $30,000 in cash for the purpose of a buy-in. The Vice President (Domestic Sales and Marketing) requested direction as to whether Crown Melbourne would allow Customer 54 to game that day. The Vice President noted Customer 54's inherent risk rating was red and his residual risk rating was black and attached a copies of company searches in respect of Customer 54 together with a patron declaration form. The declaration stated that Customer 54's wealth was under $500,000 and his source of wealth was his businesses ownership, investments and savings. Customer 54's business exported goods overseas. A short time later, the Executive General Manager (Table Games) confirmed that, based on the information attached to the email, Customer 54 could buy-in.

On 30 November 2020, the CTRM, in conjunction with the Responsible Gaming Office Coordinator, determined to prepare an SMR based on the fact that the documents indicated that Customer 54's wealth was under $500,000 which raised concerns about his losses.

On 30 November 2020, the Gaming Integrity Manager, became aware that Crown Melbourne did not have information about Customer 54's company and that Customer 54's play in the previous year was higher than the income stated on the patron declaration form. The Gaming Integrity Manager identified that Customer 54's risk rating was "red" after he attempted to withdraw funds without attributed play, and for concerns regarding "AML behaviour and associate". He noted that Crown Melbourne needed to be careful about letting some players back too soon or without time to properly review and holistically consider the individual circumstances of the players.

The Gaming Integrity Manager also identified that the domestic sales and marketing team had a vested interest in getting players back on site and it was likely not the best approach to have them sitting in on discussions about SOWs in the future.

The Executive General Manager (Table Games) recommended Crown Melbourne get updated evidence of Customer 54's domicile. On 30 November 2020, Crown Melbourne obtained a bank statement from Customer 54. On 23 December 2020, Crown Melbourne obtained a copy of a boarding pass in Customer 54's name for a domestic flight in December 2020.

Despite the concerns raised and the ML/TF risks posed and identified by senior management, Crown Melbourne continued to provide designated services to Customer 54.

Senior management engagement – February – March 2021 review

In February 2021, Customer 54 played on a domestic program and was funding his activity his significant cash buy-ins.

On 21 February 2021, the Group Senior Manager AML (Customer Intelligence and Due Diligence) requested further information about Customer 54. The Group Senior Manager AML repeated the concerns raised during the November 2020 review and added that Customer 54's patron declaration form provided a Victorian address but Crown Melbourne had accepted a boarding pass to Hobart as proof of domicile.

On 22 February 2021, Gaming Integrity Manager emailed the Vice President (Domestic Sales and Marketing). The Gaming Integrity Manager raised the Group Senior Manager AML's concerns and stated that Crown Melbourne needed further information from Customer 54 to substantiate his domicile and his source of wealth as all Crown Melbourne had was an old utility bill and a boarding pass for a Tasmanian flight. Searches conducted on the same day confirmed that Customer 54 was not on the title for the property listed on his Tasmanian driver's licence.

On 3 March 2021, Gaming Integrity Manager emailed the Vice President (Domestic Sales and Marketing). The Gaming Integrity manager reiterated that Customer 54's losses for 2018 to 2020 were well in excess of his stated income.

The Vice President (Domestic Sales and Marketing) responded asking if it would be sufficient if another source of wealth document was completed with more details and supporting evidence. The Gaming Integrity Manager responded that it was unlikely that another source of wealth form would satisfy where Customer 54's funds were actually coming from given the evidence Crown Melbourne already had on file.

On 5 March 2021, Gaming Integrity Manager emailed the Vice President (Domestic Sales and Marketing) requesting an update on Customer 54. He noted suspicion in respect of Customer 54's alleged domicile and stated that unless the Vice President's team identified information to explain the suspicion in respect of Customer 54 he would recommend that Customer 54 be prevented from attending Crown Melbourne until he provided documentation of his domicile and source of wealth.

The Vice President (Domestic Sales and Marketing) responded stating that Customer 54 would not provide any further information regarding his source of wealth.

Despite the concerns raised and the ML/TF risks posed and identified by senior management, Crown Melbourne continued to provide designated services to Customer 54.

Senior management engagement – escalation to POI Committee

On 9 March 2021, Customer 54 was escalated to the POI committee.

On 19 March 2019, the Vice President (Domestic Sales and Marketing) emailed the Gaming Integrity Manager regarding Customer 54. He advised that Customer 54 was in the process of being converted to a local Crown Rewards member. He asked the Gaming Integrity Manager to let him know if there were any problems with this before they finalised the handover to another team.

The Gaming Integrity Manager responded noting that there were still doubts about Customer 54's domicile and source of wealth, and that he had been referred to the POI Committee.

Despite the concerns raised and the ML/TF risks posed and identified by senior management, Crown Melbourne continued to provide designated services to Customer 54.

Senior management engagement – April 2021 review

On 21 April 2021, Customer 54 provided a copy of a utility bill in his name. On the same day, the Gaming Integrity Manager requested one of his team members to prepare a review of Customer 54's information. The review found:

- Customer 54 had disproportionate levels of play compared to his declared income;
- Customer 54's source of wealth was unverifiable;
- Customer 54 had played all but six days in April to date, and over 64% of the year to date. This brought into question his domicile in Tasmania;
- the boarding ticket for the flight to Hobart on 10 December 2021 did not align with his rated gaming play. He played in the Mahogany room at 10:52pm that evening. This suggested that he either purchased a ticket solely for the purpose of presenting it as false evidence of domicile, or caught a flight back to Melbourne from Hobart after leaving at 9:40 that morning so that he could play in the Mahogany room that evening; and
- the utility bill provided by Customer 54 as evidence of his Tasmanian address appeared to be doctored. The staff member expressed concern at "the apparent wilful deceitfulness of providing a falsified utility bill as evidence."

On 21 April 2021, the Gaming Integrity Manager sent the Executive General Manager – Table Games a copy of the falsified utility bill and noted that the Vice President (Domestic Sales and Marketing) had ignored his concerns regarding Customer 54's source of wealth and the disparity between his income and rated play levels. The Vice President (Domestic Sales and Marketing) had not attempted to gather any information in support of Customer 54's source of wealth.

On 30 April 2021, the Surveillance Department completed a review of Customer 54's connection to Person 53, which found:

- they both had the same Tasmanian address listed on the Crown Rewards account. There was no overlap where both individuals had that address at the same time. The property was last sold in 2013;
- they both had addresses in a Victorian suburb in close proximity to each other; and
- discrepancies on the falsified gas bill suggested that it was likely originally a bill from a gas provider located in an suburb adjacent to Customer 54's and Person 53's suburb in Victoria.

Despite the concerns raised and the ML/TF risks posed and identified by senior management, Crown Melbourne continued to provide designated services to Customer 54.

Senior management engaged – decision to issue WOL

On 4 May 2021, a Group AML Analyst prepared a Critical Risk Customer Escalation Form in respect of Customer 54 which identified the following risks:

- Customer 54's source of wealth was not commensurate with his gaming activity.
- Customer 54 had refused to provide additional supporting information to substantiate the business nature or operation of the company of which he was a director;
- there was strong evidence that Customer 54 had falsified his domicile status to access incentives programs for domestic players, including supplying falsified documentation;
- Customer 54's activity was funded exclusively through cash and he made repeated requests for gaming cheques. The review noted that this indicated a heightened ML risk of possible attempts to legitimise cash as winnings; and
- Customer 54 was linked to a banned customer who was subject to a law enforcement inquiry in relation to a money laundering investigation.

In May 2021, Group Senior Manager AML (Customer Intelligence and Due Diligence) emailed senior management a copy of the critical risk customer escalation form and recommended exiting Customer 54 from the business.

On 13 May 2021, Crown Melbourne issued a WOL in respect of Customer 54.

Enhanced customer due diligence

1907. Having formed a suspicion for the purposes of s41 of the Act, Crown Melbourne gave the AUSTRAC CEO SMRs with respect to Customer 54 on:

a. 11 December 2018;

b. 4 April 2019;

c. 3 July 2019;

d. 2 December 2020;

e. 15 January 2021; and

f. 31 January 2022.

Particulars

Each of the SMRs from 2018 to 2020:

- reported Customer 54's annual losses and average bet;
- noted threshold transactions; and
- stated that Crown Melbourne's suspicion was based on Customer 54's annual losses and the amounts of cash he was prepared to carry.

The 15 January 2021 and 31 January 2022 SMRs comprised Crown Melbourne's lookback in respect to Customer 54.

1908. On each occasion that Crown Melbourne formed a suspicion with respect to Customer 54 for the purposes of s41 of the Act, it was required to apply its ECDD program to Customer 54.

Particulars

Rule 15.9(3) of the Rules.

1909. Crown Melbourne did not carry out appropriate risk-based ECDD measures with respect to Customer 54 on each occasion that Crown Melbourne formed a suspicion with respect to Customer 54 for the purposes of s41 of the Act.

a. There are no records of ECDD being conducted following the lodgement of any SMRs: see paragraphs 664 and 685.

b. Until April 2021, appropriate risk-based steps were not taken to obtain or analyse information about Customer 54's source of wealth/funds: see paragraph 667.

c. Appropriate risk-based steps were not taken to analyse and monitor Customer 54's transactions – both past and future – including to understand their economic purpose: see paragraphs 590 and 666.

d. On each occasion prior to May 2021 that senior management considered whether to continue the business relationship with Customer 54, senior management failed to give adequate consideration to whether the ML/TF risks posed by Customer 54 were within Crown Melbourne's risk appetite: see paragraph 668ff.

Particulars

Rules 15.9(3), 15.10(1)(c), (d), (2), (5) and (6) of the Rules.

See particulars to paragraph 1906.

1910. On and from 1 December 2020, Crown Melbourne rated Customer 54 as high risk.

Particulars

Between 1 December 2020 and 11 May 2021, Crown Melbourne rated Customer 54's risk to be high on six occasions: see paragraph 1901.

1911. On each occasion that Crown Melbourne rated Customer 54 high risk, Crown Melbourne was required to apply its ECDD program to Customer 54.

Particulars

Rule 15.9(1) of the Rules.

See paragraph 661.

1912. Crown Melbourne did not carry out appropriate risk-based ECDD measures with respect to Customer 54 on each occasion that Crown Melbourne rated Customer 54 high risk.

Particulars

See paragraphs 1906 and 1909.

See paragraphs 661, 666, 667 and 668.

1913. By reason of the matters pleaded from paragraphs 1899 to 1912, on and from December 2020, Crown Melbourne:

a. did not monitor Customer 54 in relation to the provision of designated services, with a view to identifying, mitigating and managing the ML/TF risks reasonably faced; and

b. did not do so in accordance with rr 15.5 and 15.9 of the Rules

1914. By reason of the matters pleaded at paragraph 1913, Crown Melbourne contravened s36(1) of the Act on and from December 2020 to 13 May 2021 with respect to Customer 54.

Particulars

Section 36(1) of the Act is a civil penalty provision: s36(2) of the Act.

Customer 55

1915. Customer 55 has been a customer of Crown Perth since 29 September 2010.

1916. From at least 29 September 2010, Crown Perth provided Customer 55 with designated services within the meaning of table 1 and table 3, s6 of the Act.

Particulars

On 29 September 2010, Customer 55 was made a gold tier member at Crown Perth.

On 25 November 2011, Crown Perth opened a DAB account and a safekeeping account (AUD) for Customer 55 which remains open.

Between 29 September 2010 and 26 January 2019, Customer 55 participated in 125 interstate programs at Crown Perth.

Customer 55 was a regular interstate player with Crown Perth between 2010 and 2019 after which he became a local Crown Perth customer.

Between 2010 and 2015, Crown Perth recorded Customer 55's cumulative individual gaming activity to be a cumulative buy-in of $5,930,535 with a loss of $1,092,875.

Between 2016 and 2021, Crown Perth recorded Customer 55's cumulative individual gaming activity to be a cumulative buy-in of $2,109,450 with a loss of $385,725.

The ML/TF risks posed by Customer 55

1917. By 1 March 2016, higher ML/TF risks were indicated by the nature and purpose of Customer 55's business relationship with Crown Perth, the nature of the transactions he had been conducting, together with the suspicions Crown Perth itself had formed with respect to Customer 55.

Particulars

Section 36(1)(a), (b) of the Act and Chapter 15 of the Rules.

SMRs

By 1 March 2016, Crown Perth had given the AUSTRAC CEO six SMRs in relation to Customer 55 – on 19 August 2010, 22 January 2013, 28 October 2014, 10 March 2015, 6 May 2015 and 27 May 2015. The SMRs reported attempts by Customer 55 to avoid reporting obligations, including registering for a membership after cashing out to ensure that no play was recorded, buying in at slightly below the threshold limit and cashing out two sums below the threshold limit before passing the total sum to another customer. The SMRs also reported that Customer 55 had insufficient recorded play to support a cash out and instances where sums were deposited and then withdrawn in its entirety on the same day.

Telegraphic transfers

Between 26 July 2013 and 17 November 2015, Customer 55 sent six outgoing telegraphic transfers totalling $176,000 to his personal bank account.

Between 17 March 2015 and 28 February 2016, Customer 55 received four telegraphic transfers totalling $140,000 from his personal account or his Crown Melbourne DAB account.

Gaming activity

Between 2010 and 2015, Crown Perth recorded Customer 55's cumulative individual gaming activity to be a loss of $1,092,875 with a cumulative buy-in of $5,930,535.

Due diligence

As at 1 March 2016, there is no record of due diligence conducted in respect of Customer 55. Crown Perth took no steps to understand

Customer 55's source of wealth/funds and whether that source was legitimate.

1918. As at 1 March 2016, Customer 55 should have been recognised by Crown Perth as a high risk customer for the reasons pleaded at paragraph 1917.

1919. It was not until 14 February 2021 that Customer 55 was rated high risk by Crown Perth.

Particulars

Until 14 February 2021, Crown Perth did not designated Customer 55 a high risk rating despite the following:

- between 2011 and 2012, his buy-in and loss escalated dramatically from $40,550 to $826,260 and $17,000 to $184,005 respectively; and
- on two occasion, Crown Perth staff observed Customer 55 attempted to avoid threshold transactions and take measures to circumvent the requirement to report transactions over $10,000. This was indicative of the ML/TF typology of structuring.

See paragraph 120.

1920. At all times on and from 1 March 2016, Customer 55 should have been recognised by Crown Perth as a high risk customer by reason of the matters pleaded at 1917, 1921, 1922, 1923 and 1925.

Particulars

Section 36(1)(a), (b) of the Act and Chapter 15 of the Rules.

1921. On and from 1 March 2016, designated services provided to Customer 55 posed higher ML/TF risks including because the provision of designated services to Customer 55 involved a combination of the following factors:

a. Customer 55 received high value financial (table 1, s6) and gaming services (table 3, s6);

b. by no later than 2021, Crown Perth recorded Customer 55's cumulative individual gaming activity to be a loss of $1,478,600 and buy-in of $8,039,985;

c. the table 3, s6, designated services provided to Customer 55 involved escalating rates of buy-in and losses;

d. large values were transferred to and from Customer 55's bank accounts and his DAB account involving designated services within the meaning of items 31 and 32, table 1, s6 of the Act;

e. Customer 55 engaged in transactions indicative of ML/TF typologies and vulnerabilities, including structuring: see paragraph 24;

f. these transactions took place against the background of:

   i. six SMRs being given to the AUSTRAC CEO by Crown Perth by 1 March 2016;

   ii. two SMRs identified conduct indicative of the ML/TF typology of structuring;

iii. by 1 March 2016, Customer 55 had on multiple occasions attempted to avoid making threshold transactions and the associated reporting obligations incident on threshold transactions;

g. by 14 February 2021, Customer 55 made over 160 threshold transactions;

h. in February 2021, made four cash buy-ins in the Pearl room totalling $10,000 comprising sums less than the threshold limit;

i. in February 2021, Customer 55 refused to complete a source of wealth/funds form when requested to do so by Crown Perth staff; and

j. by reason of the matters set out at subparagraphs a. to i. above, there were higher ML/TF risks associated with Customer 55's source of wealth/funds.

Monitoring of Customer 55's transactions

1922. At no time did Crown Perth appropriately monitor Customer 55's transactions on a risk-basis.

Particulars

Section 36(1)(a), (b) of the Act and Rules 15.4 to 15.8 of the Rules.

Crown Perth did not apply appropriate risk-based transaction monitoring to designated services provided to Customer 55: see paragraphs 590ff and 629 to 642.

Customer 55's transactions involved repeated transactions indicative of ML/TF typologies and vulnerabilities that were not detected prior to a 2021 look-back. Had appropriate risk-based transaction monitoring been applied, these transactions could have been identified earlier: see paragraphs 686 and 687.

Transactions involving Customer 55 were identified as indicative of the ML/TF typology of structuring in his DAB account by an independent auditor in 2021. Between 16 and 25 January 2021, Customer 55 made seven cash deposits totalling $55,000 made up of transactions with values of less than $10,000.

Ongoing customer due diligence

1923. On and from 1 March 2016, on multiple occasions, the provision of designated services to Customer 55 by Crown Perth raised red flags reflective of higher ML/TF risks as a result of complex, unusually large transactions and unusual patterns of transactions which had no apparent economic or visible lawful purpose.

Particulars

See paragraph 420ff, 450 and 451.

Between 18 August 2010 and 14 February 2021, Customer 55 made over 160 threshold transactions. These mainly comprised chip redemptions or deposits and withdrawals into his DAB account.

Between 5 March 2016 and 27 January 2019, Customer 55 received 26 telegraphic transfers totalling $703,500 from his from his personal account or his Crown Melbourne DAB account.

On 28 March 2016, Crown Perth issued a $70,000 gaming cheque for Customer 55. Customer 55 redeemed $60,000 of it on the same day.

In 2016, Crown Perth recorded Customer 55's individual rated gaming activity as buy-in $1,097,650 and loss $181,850. No further details were recorded by Crown Perth in respect of Customer 55's gaming activity in 2016.

In 2017, Crown Perth recorded Customer 55's individual rated gaming activity as buy-in $122,500 and loss $32,680. No further details were recorded by Crown Perth in respect of Customer 55's gaming activity in 2017.

In 2018, Crown Perth recorded Customer 55's individual rated gaming activity as buy-in $510,900 and loss $128,855. No further details were recorded by Crown Perth in respect of Customer 55's gaming activity in 2018.

In 2019, Crown Perth recorded Customer 55's individual rated gaming activity as buy-in $186,500 and loss $69,100. No further details were recorded by Crown Perth in respect of Customer 55's gaming activity in 2019.

In 2020, Crown Perth recorded Customer 55's individual rated gaming activity as buy-in $32,000 and loss $10,600. No further details were recorded by Crown Perth in respect of Customer 55's gaming activity in 2020.

On 14 February 2021, Customer 55 attended the Pearl room Cage and deposited $10,000 into his DAB account. Customer 55 then withdrew the funds in the form of a CPV. Shortly afterwards, Customer 55 presented a further $10,000 to the Pearl room Cage for deposit: SMR dated 11 March 2021

On 14 February 2021, Customer 55 refused to complete a source of wealth form when requested to do so by Crown Perth staff in the Pearl room: SMR dated 11 March 2021.

On 14 February 2021, Customer 55 advised the Crown Perth staff that he would buy-in under $10,000 at the gaming tables. Customer 55 then made four cash buy-ins totalling $10,000 comprising sums less than the threshold limit: SMR dated 11 March 2021

In 2021, Crown Perth recorded Customer 55's individual rated gaming activity as buy-in $159,900 and win $37,360.

1924. At no time did Crown Perth undertake appropriate risk-based customer due diligence with respect to Customer 55 with a view to identifying, mitigating and managing the ML/TF risks posed by the provision of designated services on and from 1 March 2016.

a. Until February 2021, Crown Perth did not take appropriate steps to understand whether Customer 55's source of wealth/funds was legitimate.

b. Until February 2021, Crown Perth did not take appropriate steps to identify or analyse the ML/TF risks of Customer 55's transactions or to consider whether they had a lawful purpose.

c. At no time did Crown Perth give appropriate consideration to whether large and high risk transactions should be processed.

d. On each occasion that senior management considered whether to continue the business relationship with Customer 55, senior management failed to give adequate consideration to whether the ML/TF risks posed by Customer 55 were within Crown Perth's risk appetite.

Particulars

Section 36(1)(a) of the Act.

No due diligence was conducted from 1 March 2016 to February 2021 despite the high ML/TF risk posed by Customer 55 pleaded at paragraphs 1917, 1921, 1922, 1923 and 1925.

In February 2021, Customer 55 refused to complete a source of wealth/funds form when requested to do so by Crown Perth staff.

In May 2021, Crown Perth applied the SPR process of Customer 55, which determined his rating to be green (-2): see particulars to paragraph 1234.

None of these steps were proportionate to the ML/TF risks reasonably posed by Customer 55 on and from 1 March 2016.

Enhanced customer due diligence

1925. Having formed a suspicion for the purposes of s41 of the Act, Crown Perth gave the AUSTRAC CEO an SMR with respect to Customer 55 on 11 March 2021.

Particulars

The SMR described Customer 55's 14 February 2021 conduct in the Pearl room: see particulars to paragraph 1923. The SMR was filed nearly a month after the conduct to which it relates occurred.

1926. On each occasion that Crown Perth formed a suspicion with respect to Customer 55 for the purposes of s41 of the Act, it was required to apply its ECDD program to Customer 55.

Particulars

Rule 15.9(3) of the Rules.

1927. Crown Perth did not carry out appropriate risk-based ECDD measures with respect to Customer 55 on each occasion that Crown Perth formed a suspicion with respect to Customer 55 for the purposes of s41 of the Act.

a. Appropriate risk-based steps were not taken to analyse information that Crown Perth had obtained about Customer 55's source of wealth/funds, including whether the source of wealth/funds was legitimate.

b. On each occasion that senior management considered whether to continue the business relationship with Customer 55, senior management failed to give adequate consideration to whether the ML/TF risks posed by Customer 55 were within Crown Perth's risk appetite. This was despite a pattern of behaviour exhibited by Customer 55 in which he attempted to avoid reporting cash transactions that he engaged in at Crown Perth or reveal the source of the cash used for gaming activity.

Particulars

Rules 15.9(3), 15.10(1)(c), (d), (2), (5) and (6) of the Rules.

After lodging the SMR dated 11 March 2021, Crown Perth carried out ECDD: Rule 15.9(3) of the Rules.

In February 2021, Crown Perth carried out land registry searches, Australian company searches, company searches in respect of companies Customer 55 was affiliated with, bankruptcy searches, risk intelligence and open source media searches in respect of Customer 55.

In February 2021, a Crown Perth Legal Officer (AML) requested information about Customer 55 from table games staff to satisfy the ECDD requirements in Crown Perth's AML/CTF program. The Manager also emailed Customer 55's host, who did not reply. In response:

- the Table Games Manager (Crown Perth) identified that Customer 55 was a Pearl room player who ordinarily played baccarat at around $1,000 per coup; and
- an Income Control Officer (Crown Perth) provided a spreadsheet summarising Customer 55's business relationship at Crown Perth. Customer 55 was identified as having two residential addresses with a high value, although neither were owned by Customer 55. Customer 55's occupation was not on file, but his directorships and other business interests were listed.

See particulars to paragraph 1924.

1928. On 14 February 2021, Crown Perth rated Customer 55 high risk.

Particulars

Crown Perth rated Customer 55's risk to be high on 14 February 2021: see paragraph 1919.

1929. On each occasion that Crown Perth rated Customer 55 high risk, Crown Perth was required to apply its ECDD program to Customer 55.

Particulars

Rule 15.9(1) of the Rules.

See paragraph 661.

1930. Crown Perth did not carry out appropriate risk-based ECDD measures with respect to Customer 55 on each occasion that Crown Perth rated Customer 55 high risk.

Particulars

See paragraphs 1924 and 1927.

See paragraphs 661, 666, 667 and 668.

1931. By reason of the matters pleaded from paragraphs 1915 to 1930, on and from 1 March 2016, Crown Perth:

a. did not monitor Customer 55 in relation to the provision of designated services, with a view to identifying, mitigating and managing the ML/TF risks reasonably faced; and

b. did not do so in accordance with rr 15.5 and 15.9 of the Rules.

1932. By reason of the matters pleaded at paragraph 1931, Crown Perth contravened s36(1) of the Act on and from 1 March 2016 with respect to Customer 55.

Particulars

Section 36(1) of the Act is a civil penalty provision: s36(2) of the Act.

Customer 56

1933. Customer 56 was a customer of Crown Melbourne from 6 March 2013 to 20 May 2016.

1934. From at least 27 September 2013 to 20 May 2016, Crown Melbourne provided Customer 56 with designated services within the meaning of table 1 and table 3, s6 of the Act.

Particulars

On 27 September 2013, Crown Melbourne made Customer 56 a premium program player.

On 15 November 2013, Crown Melbourne opened a DAB account and a safekeeping account for Customer 56.

By the end of 2013, Crown Melbourne recorded that Customer 56's annual wins at Crown Melbourne for that year had reached $1,590,325.

By the end of 2014, Crown Melbourne recorded that Customer 56's annual losses at Crown Melbourne for that year had reached $4,080,655.

By the end of 2015, Crown Melbourne recorded that Customer 56's annual losses at Crown Melbourne for that year had reached $500,125.

By April 2016, Crown Melbourne recorded that Customer 56's annual losses at Crown Melbourne for that year had reached $367,350.

On 20 May 2016, Crown Melbourne issued an indefinite WOL against Customer 56.

The ML/TF risks posed by Customer 56

1935. By 1 March 2016 higher ML/TF risks were indicated by the nature and purpose of Customer 56's business relationship with Crown Melbourne, the nature of the transactions he had been conducting, together with the suspicions Crown Melbourne itself had formed with respect to Customer 56.

Particulars

Section 36(1)(a), (b) of the Act and Chapter 15 of the Rules.

SMRs by 1 March 2016

By 1 March 2016, Crown Melbourne had given the AUSTRAC CEO eight SMRs in relation to Customer 56 on 22 November 2013, 5 December 2013, 22 January 2014, 23 January 2014, 27 March 2014, 8 July 2014, 29 September 2014, 22 April 2015.

The majority of the SMRs reported suspicions formed relating to the threshold transactions noted for Customer 56, amounts of cash Customer 56 was prepared to carry and his annual wins and losses, as follows:

By 22 November 2013, Crown Melbourne had formed suspicions with respect to Customer 56's attendance at Crown Melbourne on 22 occasions, with total buy-ins of $447,855, average bets of $5,518 and annual wins that had already reached $106,540: SMR dated 22 November 2013.

By 5 December 2013, Crown Melbourne had formed further suspicions, as Customer 56 had attended Crown Melbourne on 32 occasions, with his total buy-in reaching $972,655, his average bet increasing to $8,453 and annual wins reaching $950,240: SMR dated 5 December 2013.

By the end of 2013, Customer 56's annual wins at Crown Melbourne had reached $1,590,325.

By 21 January 2014, Customer 56's annual wins at Crown Melbourne for 2014 had reached $4,561,930.

By 21 January 2014, Crown Melbourne had formed suspicions with respect to Customer 56, noting that it was reported he was not involved in business but residential property investments, he owed money to people in Queensland in 2013, and despite wins at other Australian casinos in 2013, Customer 56 had since lost those winnings: SMR dated 22 January 2014.

On 22 January 2014, Crown Melbourne had formed suspicions that Customer 56 was associated with another Crown patron: SMR dated 23 January 2014.

By 27 March 2014, Customer 56 had lost the money he had won in January 2014, and his annual losses had reached $1,577,015. Crown Melbourne had formed suspicions regarding his average bet increasing from $8,595 in 2013 to $104,838 in 2014: SMR dated 27 March 2014.

By 8 July 2014, Customer 56's annual losses at Crown Melbourne for 2014 had reached $2,922,015: SMR dated 8 July 2014.

On 8 July 2014, Crown Melbourne reported that a car sales company had requested to send $330,000 to Customer 56's DAB account, which formed the proceeds of a trade-in completed by Customer 56. Crown Melbourne advised the company not to transfer the funds: SMR dated 8 July 2014.

By 29 September 2014, Customer 56's annual losses at Crown Melbourne for 2014 had reached $3,571,715: SMR dated 29 September 2014.

On 28 September 2014, Crown Melbourne had formed suspicions that Customer 56 was associated with another Crown patron, Person 60. There was a deposit of $390,000 cash at Crown Melbourne associated with these customers: SMR dated 29 September 2014.

By the end of 2014, Customer 56's annual losses at Crown Melbourne for 2014 had reached $4,080,655: SMR dated 22 April 2015.

On 22 April 2015, the Crown patron Person 60 transferred $75,000 from his DAB account to Customer 56's DAB account.

By 22 April 2015, Crown Melbourne reported that it continued to suspect that Customer 56 was associated with Crown patron Person 60. It had also formed suspicions with respect to Customer 56's average bet increasing from $8,959 in 2013 to $59,724 in 2014: SMR dated 22 April 2015.

Law enforcement inquiries by 1 March 2016

On 25 March 2014, Crown Melbourne was notified that Customer 56 was the subject of law enforcement interest in a drug trafficking and money laundering investigation.

On 9 April 2014, Crown Melbourne was notified that Customer 56 was a subject of law enforcement interest in a separate drug trafficking and money laundering investigation.

Due diligence conducted by 1 March 2016

At no time prior to 1 March 2016, did Crown Melbourne take any due diligence steps with respect to Customer 56.

1936. As at 1 March 2016, Customer 56 should have been recognised by Crown Melbourne as a high risk customer for the reasons pleaded at paragraph 1935.

Particulars

Section 36(1)(a), (b) of the Act and Chapter 15 of the Rules.

1937. At all times on and from 1 March 2016, Customer 56 should have been recognised by Crown Melbourne as a high risk customer by reason of the matters pleaded at paragraphs 1935, 1939, 1941 and 1943.

Particulars

Section 36(1)(a), (b) of the Act and Chapter 15 of the Rules.

1938. It was not until 26 May 2016 that Customer 56 was rated high risk by Crown Melbourne.

Particulars

On 22 November 2013, Crown Melbourne assessed Customer 56 as moderate risk.

On 21 January 2014, Crown Melbourne assessed Customer 56 as significant risk.

See paragraph 120.

1939. On and from 1 March 2016, designated services provided to Customer 56 posed higher ML/TF risks including because the provision of designated services to Customer 56 involved a combination of the following factors:

a. Customer 56 received high value financial (table 1, s6) and gaming services (table 3, s6);

b. Customer 56 transacted using large amounts of cash and cash that appeared suspicious, including counterfeit cash: see paragraphs 450, 451 and 452;

c. the table 3, s6, designated services provided to Customer 56 involved high wins and high losses;

d. large values were transferred to Customer 56's DAB account from other customers' DAB accounts, involving the provision by Crown Melbourne of designated services within the meaning of items 31 and 32, table 1, s6 of the Act;

e. these transactions took place against the background of:

i. law enforcement having expressed an interest in Customer 56 on two occasions in 2014;

ii. eight SMRs being given to the AUSTRAC CEO by Crown Melbourne by 1 March 2016;

iii. Customer 56's average bet increasing exponentially from $8,595 in 2013 to $104,838 in 2014;

iv. Customer 56 having no clear source of funds or source of wealth to justify his large spend;

v. Customer 56 having engaged in a high number of transactions that Crown Melbourne identified and reported as suspicious;

f. in 2016, Customer 56 was the subject of law enforcement inquiries in relation to drug trafficking and money laundering on two occasions;

g. on 19 May 2016, Customer 56 was arrested and charged with a firearms offence; and

h. by reason of the matters set out at subparagraphs a. to g. above, there were real risks that Customer 56's source of wealth/funds were not legitimate.

Monitoring of Customer 56's transactions

1940. At no time did Crown Melbourne appropriately monitor Customer 56's transactions on a risk-basis.

Particulars

Section 36(1)(a), (b) of the Act and Rules 15.4 to 15.8 of the Rules.

Crown Melbourne did not apply appropriate risk-based transaction monitoring to designated services provided to Customer 56: see paragraphs 590ff and 629 to 642.

Ongoing customer due diligence

1941. On and from 1 March 2016, on multiple occasions, the provision of designated services to Customer 56 by Crown Melbourne raised red flags reflective of higher ML/TF risks.

Particulars

During the following times, designated services provided to Customer 56 involved complex, unusually large transactions and unusual patterns of transactions which had no apparent economic or visible lawful purpose.

On 26 April 2016, Crown Melbourne suspected that Customer 56 had presented two counterfeit $50 notes: SMR dated 27 April 2016.

By 26 April 2016, Customer 56's annual losses for that year had already reached $500,125.

On 12 May 2016 and 13 May 2016, Crown Melbourne received two law enforcement enquiries with respect to Customer 56 as part of an investigation into drug trafficking and money laundering.

On 19 May 2016, Customer 56 was arrested by a law enforcement agency at Crown Towers and charged with a firearms offence.

On 20 May 2016, Crown Melbourne received a further law enforcement inquiry with respect to Customer 56.

1942. At no time did Crown Melbourne undertake appropriate risk-based customer due diligence with respect to Customer 56 with a view to identifying, mitigating and managing the ML/TF risks posed by the provision of designated services on and from 1 March 2016.

a. Prior to 20 May 2016, Crown Melbourne did not undertake any due diligence steps with respect to Customer 56 despite:

    i. giving the AUSTRAC CEO two SMRs relating to Customer 56, which indicated Crown Melbourne was suspicious of Customer 56's association with other Crown patrons and Customer 56 presenting suspected counterfeit notes at Crown Melbourne; and

    ii. law enforcement requesting information relating to Customer 56 on a number of occasions.

b. At no time did Crown Melbourne take appropriate steps to understand whether Customer 56's source of wealth/funds was legitimate.

c. At no time did Crown Melbourne take appropriate steps to identify or analyse the ML/TF risks of Customer 56's transactions or to consider whether they had a lawful purpose.

d. Crown Melbourne gave no consideration at any time on and from 1 March 2016 to whether large and high risk transactions should be processed.

e. Prior to the decision to issue Customer 56 with a WOL in May 2016, there is no record of senior management considering whether continuing the business relationship with Customer 56 was within Crown Melbourne's ML/TF risk appetite in light of the ML/TF risks posed by Customer 56.

Particulars

Rules 15.9(3), 15.10(1)(c), (d), (2), (5) and (6) of the Rules.

At no time did Crown Melbourne take any due diligence steps taken with respect to Customer 56. This was not proportionate to the ML/TF risks reasonably posed by Customer 56 on and from 1 March 2016.

On 20 May 2016, in response to his arrest, Crown Melbourne issued Customer 56 with a WOL.

Enhanced customer due diligence

1943. Having formed a suspicion for the purposes of s41 of the Act, Crown Melbourne gave the AUSTRAC CEO SMRs with respect to Customer 56 on:

a. 27 April 2016; and

b. 2 June 2016.

Particulars

The SMRs reported suspicions related to the presentation of counterfeit notes and Customer 56's associations with other Crown patrons.

1944. On each occasion that Crown Melbourne formed a suspicion with respect to Customer 56 for the purposes of s41 of the Act, it was required to apply its ECDD program to Customer 56.

Particulars

Rule 15.9(3) of the Rules.

1945. Crown Melbourne did not carry out appropriate risk-based ECDD measures with respect to Customer 56 on each occasion that Crown Melbourne formed a suspicion with respect to Customer 56 for the purposes of s41 of the Act.

a. There are no records of ECDD being conducted following the lodgement of SMRs on 27 April 2016: see paragraphs 664 and 685. The 2 June 2016 was given to the AUSTRAC CEO after Crown Melbourne issued a WOL in respect of Customer 56.

b. Appropriate risk-based steps were not taken to obtain or analyse information about Customer 56's source of wealth/funds: see paragraph 667.

c. Appropriate risk-based steps were not taken to analyse and monitor Customer 56's transactions – both past and future – including to understand their economic purpose: see paragraphs 590 and 666.

d. Prior to the decision to issue Customer 56 with a WOL in May 2016, there is no record of senior management considering whether continuing the business relationship with Customer 56 was within Crown Melbourne's ML/TF risk appetite in light of the ML/TF risks posed by Customer 56: see paragraph 668ff.

Particulars

Rules 15.9(3), 15.10(1)(c), (d), (2), (5) and (6) of the Rules.

See particulars to paragraph 1942.

1946. By reason of the matters pleaded from paragraphs 1933 to 1945, on and from 1 March 2016, Crown Melbourne:

a. did not monitor Customer 56 in relation to the provision of designated services, with a view to identifying, mitigating and managing the ML/TF risks reasonably faced; and

b. did not do so in accordance with rr 15.5 and 15.9 of the Rules.

1947. By reason of the matters pleaded at paragraph 1946, Crown Melbourne contravened s36(1) of the Act on and from 1 March 2016 to 20 May 2016 with respect to Customer 56.

Particulars

Section 36(1) of the Act is a civil penalty provision: s36(2) of the Act.

Customer 57

1948. Customer 57 was a customer of Crown Melbourne from 24 April 1996 to 5 December 2019.

1949. From at least 22 September 2007 to December 2019, Crown Melbourne provided Customer 57 with designated services within the meaning of table 3, s6 of the Act.

1950. From at least 22 September 2007 to 23 November 2017, Crown Melbourne provided Customer 57 with designated services within the meaning of table 1, s6 of the Act.

Particulars to paragraphs 1949 and 1950

On 22 September 2007, Crown Melbourne opened a DAB account for Customer 57 which remains open.

On 4 December 2016, Crown Melbourne opened a CCF account (AUD) for Customer 57, which was closed on 23 November 2017.

Customer 57 regularly used electronic gaming machines at Crown Melbourne.

Between 2002 and 2015, Crown Melbourne recorded Customer 57's individual rated gaming activity to be a cumulative loss of $166,013.

Between 2016 and 2019, Crown Melbourne recorded Customer 57's individual rated gaming activity to be a cumulative loss of $126,161.

On 5 December 2019, Crown Melbourne issued an indefinite WOL in respect of Customer 57.

The ML/TF risks posed by Customer 57

1951. By July 2014, Crown Melbourne were aware that there were real and significant doubts as to the legitimacy of Customer 57's funds after receiving an enquiry from an Australian corruption commission.

Particulars

On 29 July 2014, Crown Melbourne was notified by an Australian corruption commission that Customer 57 was a person of interest in an investigation, which related to three other persons of interest and possible offending dating from 1996 to 2014

1952. By April 2015, Crown Melbourne were aware that media articles had named Customer 57 in connection with an Australian corruption commission investigation into alleged misappropriation of public funds.

Particulars

Section 36(1)(a), (b) of the Act and Chapter 15 of the Rules.

By 1 March 2016, Crown Melbourne had given the AUSTRAC CEO an SMR in relation to Customer 57 on 28 April 2015. The SMR reported that Customer 57 was named in a newspaper article related to an Australian corruption commission investigation into the alleged misappropriation of public funds. The SMR also reported of Customer 57's annual losses from 2011-2015.

Following the SMR, Crown Melbourne collated Customer 57's SYCO records, a copy of Customer 57's Victorian driver's licence and results from a land registry search. Crown Melbourne also conducted an Australian company search.

1953. As at 1 March 2016, there were real and significant doubts as to the legitimacy of Customer 57's funds for the reasons pleaded at paragraphs 1951 and 1952. At all times on and from 1 March 2016, Customer 57 should have been recognised by Crown Melbourne as a high risk customer

Particulars

Section 36(1)(a), (b) of the Act and Chapter 15 of the Rules.

1954. It was not until 23 November 2017 that Customer 57 was rated high risk by Crown Melbourne.

Particulars

On 30 December 2016, Customer 57 was assessed as moderate risk.

On various occasions between 30 July 2014 and 28 April 2015, Crown Melbourne assessed Customer 57 as significant risk.

This was despite Crown Melbourne being aware that Customer 57 was implicated in allegations of misappropriation of public funds.

On various occasions between 23 November 2017 and 6 December 2019, Crown Melbourne assessed Customer 57 as high risk.

See paragraph 120.

1955. On and from 1 March 2016 designated services provided to Customer 57 posed higher ML/TF risks including because the provision of designated services to Customer 57 involved a combination of the following factors:

a. Customer 57 received high value financial (table 1, s6) and gaming services (table 3, s6);

b. by 2019, Crown Melbourne recorded Customer 57's individual rated gaming activity to be a cumulative loss of $292,174;

c. these transactions took place against the background of:

i. on 29 July 2014, Crown Melbourne was notified by an Australian corruption commission that Customer 57 was a person of interest in an investigation, which related to three other persons of interest and possible offending dating from 1996 to 2014;

ii. by 28 April 2015, Crown Melbourne were aware that media reports relating to an Australian corruption commission investigation regarding the misappropriation of public funds had named Customer 57;

d. notwithstanding that Crown Melbourne was aware that there were real and significant doubts as to the legitimacy of Customer 57's funds, Crown Melbourne nevertheless opened a CCF in December 2016. Shortly after this, in January 2017, Customer 57 was charged with conspiracy to defraud and dealing in proceeds of crime ($300,000);

e. by 23 November 2017 Crown Melbourne was aware of media reports naming Customer 57 as being charged with conspiracy to defraud and dealing in proceeds of crime ($300,000) in January 2017. In July 2021, Customer 57 was convicted and sentenced to a two-year and five months term of imprisonment; and

f. by reason of the matters set out at subparagraphs a. to e. above, there were real risks that Customer 57's source of wealth and source of funds were not legitimate.

Monitoring of Customer 57's transactions

1956. At no time did Crown Melbourne appropriately monitor Customer 57's transactions on a risk-basis.

Particulars

Section 36(1)(a), (b) of the Act and Rules 15.4 to 15.8 of the Rules.

Despite Crown Melbourne's knowledge that there were real and significant doubts as to whether Customer 57's funds were legitimate, Crown Melbourne did not apply appropriate risk-based transaction monitoring to designated services provided to Customer 57: see paragraphs 590ff and 629 to 642.

Moreover, on 4 December 2016, Crown Melbourne opened a CCF account (AUD) for Customer 57.

Ongoing customer due diligence

1957. On and from 1 March 2016, despite Crown Melbourne's knowledge that Customer 57 was named in 2015 in connection with an Australian corruption commission investigation into alleged misappropriation of public funds and charged in 2017 with conspiracy to defraud and dealing in proceeds of crime, Crown Melbourne continued to provide designated services to Customer 57.

Particulars

From 2016 to 2019, Customer 57's cumulative loss was $126,161.

By 23 November 2017 Crown Melbourne was aware of media reports naming Customer 57 as being charged with conspiracy to defraud and dealing in proceeds of crime ($300,000) in January 2017.

Despite this, on and from November 2017, Crown Melbourne continued to provide designated services to Customer 57. From November 2017 to 2019, Customer 57 had losses totalling approximately $18,000.

1958. At no time did Crown Melbourne undertake appropriate risk-based customer due diligence with respect to Customer 57 with a view to identifying, mitigating and managing the ML/TF risks posed by the provision of designated services on and from 1 March 2016.

a. Despite Crown Melbourne's knowledge that there were real and significant doubts as to the legitimacy of Customer 57's funds, at no time did Crown Melbourne take appropriate steps to understand Customer 57's source of wealth/funds.

b. At no time did Crown Melbourne take appropriate steps to identify or analyse the ML/TF risks of Customer 57's transactions or to consider whether they had a lawful purpose.

c. Prior to the decision to issue Customer 57 with a WOL in December 2019, there is no record of senior management considering whether continuing the business relationship with Customer 56 was within Crown Melbourne's ML/TF risk appetite in light of the ML/TF risks posed by Customer 57.

Particulars

Section 36(1)(a) of the Act.

At no time did Crown Melbourne take appropriate steps to establish that the source of Customer 57's funds were legitimate.

In September 2016 and November 2017, Crown Melbourne conducted a risk intelligence search in respect of Customer 57. The November 2017 search named Customer 57 as being charged with conspiracy to defraud and dealing in the proceeds of crime.

Had Crown Melbourne been conducting appropriate risk-based ongoing due diligence, they likely would have become aware of the January 2017 charge prior to the November 2017 search. Nonetheless, Crown Melbourne did not issue a WOL in respect of Customer 57 until December 2019.

In November 2019, Crown Melbourne conducted a number of database searches in relation to Customer 57 including a risk intelligence search. A media report search returned 22 articles. Each of the articles related to the Australian corruption commission inquiry and subsequent criminal proceedings.

The articles were dated between 27 April 2015 and 30 December 2018, and reported on allegations relating to Customer 57 dating back to 1996. One of the articles reported that Customer 57 had admitted to creating a false paper trail with another person of interest to try and justify hundreds of thousands of dollars in public funds to businesses he owned. Another of the articles reported that Customer 57 had been charged. Six of the articles, dated 25 January 2017 to 30 December 2018, reported on the court proceedings.

None of these steps were proportionate to the ML/TF risks reasonably posed by Customer 57 on and from 1 March 2016.

On 5 December 2019, Crown Melbourne issued an indefinite WOL in respect of Customer 57.

Enhanced customer due diligence

1959. Having formed a suspicion for the purposes of s41 of the Act, Crown Melbourne gave the AUSTRAC CEO SMRs with respect to Customer 57 on 24 November 2017.

Particulars

The grounds for suspicion for the SMR given to the AUSTRAC CEO on 24 November 2017 were that there was a person with the same name as Customer 57 recorded in a risk intelligence search as having been charged in January 2017 with conspiracy to defraud and dealing in the proceeds of crime (AUD300,000) and the case was adjourned to July 2017. The grounds also included Customer 57's rated gaming activity in the period 2011-2017.

1960. On each occasion that Crown Melbourne formed a suspicion with respect to Customer 57 for the purposes of s41 of the Act, it was required to apply its ECDD program to Customer 57.

Particulars

Rule 15.9(3) of the Rules.

1961. Crown Melbourne did not carry out appropriate risk-based ECDD measures with respect to Customer 57 on each occasion that Crown Melbourne formed a suspicion with respect to Customer 57 for the purposes of s41 of the Act.

a. There are no records of ECDD being conducted following the lodgement of SMRs on 24 November 2017, despite Crown Melbourne having knowledge that he had been charged with conspiracy to defraud and dealing with the proceeds of crime: see paragraphs 664 and 685.

b. Appropriate risk-based steps were not taken to analyse and monitor Customer 57's transactions – both past and future – including to understand their economic purpose: see paragraphs 590 and 666.

c. Prior to the decision to issue Customer 57 with a WOL in December 2019, there is no record of senior management considering whether continuing the business relationship with Customer 56 was within Crown Melbourne's ML/TF risk appetite in light of the ML/TF risks posed by Customer 57: see paragraph 668ff.

Particulars

Rules 15.9(3), 15.10(1)(c), (d), (2), (5) and (6) of the Rules.

In November 2017, Crown Melbourne conducted a risk intelligence search in respect of Customer 57 which named Customer 57 as being charged with conspiracy to defraud and dealing in the proceeds of crime. No other steps were taken to identifying, mitigating and managing the ML/TF risk reasonably posed by Customer 57.

Se particulars to paragraph 1958.

1962. On and from 23 November 2017, Crown Melbourne rated Customer 57 high risk.

Particulars

Crown Melbourne rated Customer 57 high risk on five occasions between 23 November 2017 and 6 December 2019: see paragraph 1954.

1963. On each occasion that Crown Melbourne rated Customer 57 high risk, Crown Melbourne was required to apply its ECDD program to Customer 57.

Particulars

Rule 15.9(1) of the Rules.

See paragraph 661.

1964. Crown Melbourne did not carry out appropriate risk-based ECDD measures with respect to Customer 57 on each occasion that Crown Melbourne rated Customer 57 high risk.

Particulars

At no time did Crown Melbourne conduct ECDD following each occasion that it rated Customer 57 high risk.

See paragraphs 1958 and 1961.

See paragraphs 661, 666, 667 and 668.

1965. By reason of the matters pleaded from paragraphs 1948 to 1964, on and from 1 March 2016, Crown Melbourne:

a. did not monitor Customer 57 in relation to the provision of designated services, with a view to identifying, mitigating and managing the ML/TF risks reasonably faced; and

b. did not do so in accordance with rr 15.5 and 15.9 of the Rules.

1966. By reason of the matters pleaded at paragraph 1965, Crown Melbourne contravened s36(1) of the Act on and from 1 March 2016 to 5 December 2019 with respect to Customer 57.

Particulars

Section 36(1) of the Act is a civil penalty provision: s36(2) of the Act.

Customer 58

1967. Customer 58 was a customer of Crown Melbourne since 3 July 2016 to June 2021.

1968. From 3 July 2016, Crown Melbourne provided Customer 58 with designated services within the meaning of table 1 and table 3, s6 of the Act.

Particulars

On 3 July 2016, Crown Melbourne opened a DAB account and a safekeeping account for Customer 58 under two PIDs.

On 3 July 2016, Crown Melbourne made Customer 58 a premium program player.

On 8 June 2021, Crown Melbourne issued a WOL in respect of Customer 58.

1969. By no later than October 2016, Customer 58 should have been recognised by Crown Melbourne as a high risk customer by reason of the matters pleaded at paragraphs 1971, 1973, 1974 and 1976.

Particulars

Section 36(1)(a), (b) of the Act and Chapter 15 of the Rules.

1970. It was not until 9 June 2021 that Crown Melbourne assessed Customer 58 as high risk.

Particulars

On various occasions between 24 August 2016 and 12 November 2018, Crown Melbourne assessed Customer 58 as moderate risk.

On 9 June 2021, Crown Melbourne assessed Customer 58's as high risk.

See paragraph 120.

The ML/TF risks posed by Customer 58

1971. At all times on and from 3 July 2016, designated services provided to Customer 58 posed higher ML/TF risks including because the provision of designated services to Customer 58 involved a combination of the following factors:

a. Customer 58 received high value financial (table 1, s6) and gaming services (table 3, s6), including through EGMs. EGMs presented high ML/TF risks: see paragraph 435;

b. the table 3, s6, designated services provided to Customer 58 involved high turnover;

c. Customer 58 carried large amounts of cash and transacted using large amounts of cash;

d. large values were transferred to and from Customer 58's bank accounts and his DAB account, involving the provision by Crown Melbourne of designated services within the meaning of items 31 and 32, table 1, s6 of the Act: see paragraph 411ff;

e. Customer 58 engaged in transactions indicative of ML/TF typologies and vulnerabilities, including structuring: see paragraph 24; and

f. by reason of the matters set out at subparagraphs a. to e. above, there were real risks that Customer 58's source of wealth/funds were not legitimate.

Monitoring of Customer 58's transactions

1972. At no time did Crown Melbourne appropriately monitor Customer 58's transactions on a risk-basis.

Particulars

Section 36(1)(a), (b) of the Act and Rules 15.4 to 15.8 of the Rules.

Crown Melbourne did not apply appropriate risk-based transaction monitoring to designated services provided to Customer 58: see paragraphs 590ff and 629 to 642.

Ongoing customer due diligence

1973. On and from 3 July 2016, on multiple occasions, the provision of designated services to Customer 58 raised red flags reflective of higher ML/TF risks arising from Customer 58's gaming activity through EGMs.

Particulars

Customer 58 was an EGM player: see paragraph 435.

Gaming activity at Crown Melbourne

From 3 July 2016 to 2020, Customer 58's cumulative turnover was $36,663,766. Customer 58's cumulative loss was $2,927,715.70.

Gaming activity in 2016

From 3 July 2018, Crown Melbourne formed suspicions about Customer 58's annual losses and the amounts of cash he was prepared to carry, giving several SMRs to the AUSTRAC CEO as follows:

- by 24 August 2016, Crown Melbourne recorded that Customer 58's annual losses had already reached a total of $109,229;
- by 7 September 2016, Crown Melbourne recorded that Customer 58's cumulative annual losses had reached a total of $341,370; and
- by 21 October 2016, when Crown Melbourne gave its third SMR, Customer 58 had accumulated $1,458,008 in annual losses since 3 July 2016. Customer 58 had also engaged in multiple large cash transactions and had won two jackpots totalling $42,796.

By the end of 2016, Crown Melbourne had recorded that Customer 58's turnover was $19,940,000, with losses totalling $1,770,000.

Gaming activity in 2017

By the end of 2017, Crown Melbourne had recorded that Customer 58's turnover was $8,700,000 with losses totalling $593,947.87.

Gaming activity in 2018

During the course of 2018, Crown Melbourne formed suspicions regarding Customer 58's annual losses and the amounts of cash he was prepared to carry.

By the end of 2018, Crown Melbourne had recorded that Customer 58's turnover was $7,190,000 with losses of $558,336.83.

Gaming activity in 2019

By the end of 2019, Crown Melbourne had recorded that Customer 58's turnover was $803,766 with losses of $5,431.

1974. On and from 3 July 2016, on multiple occasions, the provision of designated services to Customer 58 raised red flags reflective of higher ML/TF risks as a result of unusual transactions and patterns of transactions involving Customer 58.

Particulars

Between 3 July 2016 and 21 April 2019, Customer 58 made 166 threshold transactions totalling $2,700,000. He had also withdrawn $22,244 in cash in increments below the reporting threshold including some in a series of transactions that appeared to be deliberately structured.

Between 19 August 2016 and 14 December 2018, Customer 58 had transferred a total of $849,000 to his DAB account from his personal accounts across 26 transactions and a total of $755,885 from Crown Melbourne to his personal accounts across six transactions.

1975. At no time did Crown Melbourne undertake appropriate risk-based customer due diligence with respect to Customer 58 with a view to identifying, mitigating and managing the ML/TF risks posed by the provision of designated services on and from 3 July 2016.

a. At no time did Crown Melbourne take appropriate steps to understand whether Customer 58's source of wealth/funds was legitimate.

b. At no time did Crown Melbourne take appropriate steps to identify or analyse the ML/TF risks of Customer 58's transactions or to consider whether they had a lawful purpose.

c. At no time did Crown Melbourne give appropriate consideration to whether large and high risk transactions should be processed.

d. Prior to the decision to issue Customer 58 with a WOL in June 2021, there is no record of senior management considering whether continuing the business relationship with Customer 58 was within Crown Melbourne's ML/TF risk appetite in light of the ML/TF risks posed by Customer 58.

Particulars

Section 36(1)(a) of the Act.

The due diligence steps taken with respect to Customer 58 included:

On 25 August 2020, Crown Melbourne performed a property search.

This step was not proportionate or responsive to the ML/TF risks reasonably posed by Customer 58 on and from 3 July 2016.

On 4 June 2021, media reports identified Customer 58 as one of three individuals arrested and charged in connection with a transnational organised criminal syndicate engaged in a conspiracy to supply cocaine with a potential street value of $900,000,000.

Following this, Customer 58 was referred to Crown Melbourne's Financial Crime team, which concluded that Customer 58 posed "a significant regulatory and reputational risk to Crown" and issued a WOL in respect of Customer 58 on 8 June 2021.

Enhanced customer due diligence

1976. Having formed a suspicion for the purposes of s41 of the Act, Crown Melbourne gave the AUSTRAC CEO SMRs with respect to Customer 58 on:

a. 24 August 2016;

b. 7 September 2016;

c. 27 September 2016;

d. 21 October 2016;

e. 1 November 2018;

f. 12 November 2018; and

g. 9 June 2021.

Particulars

Each of these SMRs given to the AUSTRAC CEO from 2016 to 2018 reported Customer 58's annual losses and the amount of cash Customer 58 was prepared to carry.

The SMR given to the AUSTRAC CEO in 2021 reported Customer 58's "intense and unusual" gaming activity and financial transactions.

1977. On each occasion that Crown Melbourne formed a suspicion with respect to Customer 58 for the purposes of s41 of the Act, it was required to apply its ECDD program to Customer 58.

Particulars

Rule 15.9(3) of the Rules.

1978. Crown Melbourne did not carry out appropriate risk-based ECDD measures with respect to Customer 58 on each occasion that Crown Melbourne formed a suspicion with respect to Customer 58 for the purposes of s41 of the Act.

a. There are no records of ECDD being conducted following the lodgement of SMRs on 24 August 2016, 7 September 2016, 27 September 2016, 21 October 2016, 1 November 2018 and 12 November 2018: see paragraphs 664 and 685.

b. Appropriate risk-based steps were not taken to obtain or analyse information about Customer 58's source of wealth/funds: see paragraph 667.

c. Appropriate risk-based steps were not taken to analyse and monitor Customer 58's transactions – both past and future – including to understand their economic purpose: see paragraphs 590 and 666.

d. Prior to the decision to issue Customer 58 with a WOL in June 2021, there is no record of senior management considering whether continuing the business relationship with Customer 58 was within Crown Melbourne's ML/TF risk appetite in light of the ML/TF risks posed by Customer 58: see paragraph 668ff.

Particulars

Rules 15.9(3), 15.10(1)(c), (d), (2), (5) and (6) of the Rules.

See particulars to paragraph 1975.

1979. By reason of the matters pleaded from paragraphs 1967 to 1978, on and from 24 August 2016, Crown Melbourne:

a. did not monitor Customer 58 in relation to the provision of designated services, with a view to identifying, mitigating and managing the ML/TF risks reasonably faced, and

b. did not do so in accordance with rr 15.5 and 15.9 of the Rules.

1980. By reason of the matters pleaded at paragraph 1979, Crown Melbourne contravened s36(1) of the Act on and from 24 August 2016 to 8 June 2021 with respect to Customer 58.

Particulars

Section 36(1) of the Act is a civil penalty provision: s36(2) of the Act.

Customer 59

1981. Customer 59 was a customer of Crown Melbourne from 6 March 2006 to 29 February 2020.

1982. From at least 2010 to 29 February 2020, Crown Melbourne provided Customer 59 with designated services within the meaning of table 3, s6 of the Act.

Particulars

By 28 January 2020, Crown Melbourne recorded that Customer 59 had accumulated $1,302,966 in annual losses.

Between 2016 and 2018, Crown Melbourne recorded that Customer 59 had received large machine payouts from EGMs totalling at least $1,406,534.

In 2018, Crown Melbourne recorded that Customer 59 had been paid $56,423 in cancel credits.

On 23 November 2020, Crown Melbourne issued a WOL in respect of Customer 59.

The ML/TF risks posed by Customer 59

1983. By 1 March 2016, higher ML/TF risks were indicated by the nature and purpose of Customer 59's business relationship with Crown Melbourne, the nature of the transactions he had been conducting, together with the suspicions Crown Melbourne itself had formed with respect to Customer 59.

Particulars

Section 36(1)(a), (b) of the Act and Chapter 15 of the Rules.

By 1 March 2016, Crown Melbourne had formed suspicions about Customer 59, submitting one SMR on 6 May 2015 that reported that Customer 59 had accumulated annual losses of $104,537 between 2011 and 2015 and was prepared to carry large amounts of cash.

By 1 March 2016, Crown Melbourne also recorded two machine payouts to Customer 59 totalling $66,462.

By 1 March 2016, law enforcement had expressed interest in Customer 59 on three occasions on 24 April 2015, 28 April 2015 and 6 May 2015.

1984. As at 1 March 2016, Customer 59 should have been recognised by Crown Melbourne as a high risk customer for the reasons pleaded at paragraph 1983.

Particulars

Section 36(1)(a), (b) and Chapter 15 of the Rules.

1985. On and from 1 March 2016, Customer 59 should have been recognised by Crown Melbourne as a high risk customer for the reasons pleaded at paragraph 1983.

Particulars

Section 36(1)(a), (b) and Chapter 15 of the Rules.

1986. It was not until 2 November 2016 that Crown Melbourne first assessed Customer 59 as high risk.

Particulars

On various occasions between 6 May 2015 and 20 July 2016, Crown Melbourne assessed Customer 59 as significant risk.

On various occasions between 2 November 2016 and 16 February 2021, Crown Melbourne assessed Customer 59 as high risk.

See paragraph 120.

1987. At all times on and from 1 March 2016, designated services provided to Customer 59 posed higher ML/TF risks including because the provision of designated services to Customer 59 involved a combination of the following factors:

a. Customer 59 received high value gaming services (table 3, s6), including through EGMs. EGMs presented higher ML/TF risks: see paragraph 435;

b. the table 3, s6, designated services provided to Customer 59 involved escalating rates of high turnover;

c. Customer 59 carried large amounts of cash and transacted using large amounts of cash;

d. Customer 59 frequently received cancel credits from EGM play, which is indicative of the ML/TF typology of quick turnover of funds (without betting);

e. these transactions took place against the background of:

   i. law enforcement having expressed an interest in Customer 59 on three occasions in 2015; and

   ii. one SMR being given to the AUSTRAC CEO by Crown Melbourne;

f. between 2016 and 2018, Customer 59 was the subject of law enforcement inquiries on ten occasions;

g. by at least July 2018, Crown Melbourne was aware that law enforcement was investigating Customer 59 in relation to suspected large-scale money laundering from proceeds of drug related activities;

h. from at least 2014 and 2019, media reports named Customer 59 as a person involved in drug trafficking of large amounts of methamphetamine and cocaine; and

i. by reason of the matters set out at subparagraphs a. to h. above, there were real risks that Customer 59's source of wealth/funds were not legitimate.

Monitoring of Customer 59's transactions

1988. At no time did Crown Melbourne appropriately monitor Customer 59's transactions on a risk-basis.

Particulars

Section 36(1)(a), (b) of the Act and Rules 15.4 to 15.8 of the Rules.

Crown Melbourne did not apply appropriate risk-based transaction monitoring to designated services provided to Customer 59, including gaming through EGMs: see paragraph 435.

Ongoing customer due diligence

1989. On and from 1 March 2016, on multiple occasions, the provision of designated services to Customer 59 raised red flags reflective of higher ML/TF risks arising from Customer 59's gaming activity through EGMs.

Particulars

Customer 59 was an EGM player: see paragraph 435.

EGM activity in 2016

Customer 59 attended Crown Melbourne on 39 occasions in 2016.

During the course of 2016, Crown Melbourne formed suspicions regarding Customer 59's annual losses and the amounts of cash he was prepared to carry.

By 20 April 2016, Crown Melbourne recorded that Customer 59's annual losses for 2016 had reached $75,578. By 3 November 2016, Crown Melbourne recorded that Customer 59's annual losses had doubled to $159,337.

On 7 October 2016, Crown Melbourne recorded a machine payout for Customer 59 in the sum of $15,614.

By the end of 2016, Crown Melbourne recorded that Customer 59's annual turnover was $1,295,344 with annual losses of $179,107.

EGM activity in 2017

Customer 59 attended Crown Melbourne on 56 occasions in 2017.

On 24 May 2017, Crown Melbourne recorded a machine payout for Customer 59 in the sum of $494,047, which was paid to Customer 59 in the form of a cheque in the sum of $400,000 and cash in the amount of $94,047.20.

On 14 June 2017, Customer 59 exchanged $29,000 in chips for cash.

Between 1 March 2017 and 18 June 2017, Crown Melbourne recorded 13 machine payouts to Customer 59 totalling $788,234.

On 10 September 2017, Crown Melbourne recorded a machine payout to Customer 59 of $15,000.90.

By the end of 2017, Crown Melbourne recorded that Customer 59's annual turnover had escalated to $2,940,498, with losses of $181,693.

EGM activity in 2018

During the course of 2018, Crown Melbourne formed suspicions regarding Customer 59's annual losses and the amounts of cash he was prepared to carry.

By 18 January 2018, Crown Melbourne reported that Customer 59 had already recorded losses totalling $10,898 for 2018.

Between 18 January 2018 and 16 July 2018, Crown Melbourne recorded 21 machine payouts to Customer 59 totalling $433,729.

By 5 June 2018, Crown Melbourne reported that his annual losses had increased to a total of $201,122.

On 11 July 2018, Crown Melbourne recorded it had paid out $34,479 in cancelled credits to Customer 59.

On 16 July 2018, Crown Melbourne recorded it had paid out $21,945 in cancelled credits to Customer 59. It also recorded machine payouts of $9,996 and $3,009 to Customer 59.

On 21 July 2018, Crown Melbourne recorded a machine payout to Customer 59 of $10,002.

On 30 July 2018, Crown Melbourne recorded a machine payout to Customer 59 of $15,091.

On 20 August 2018, Crown Melbourne recorded two machine payouts to Customer 59 totalling $37,136.

On 22 August 2018, Crown Melbourne recorded a machine payout to Customer 59 of $24,476.

By 29 August 2018, Customer 59's annual losses had reached $304,419.

On 24 September 2018, Crown Melbourne recorded two machine payouts to Customer 59 of $24,240.20 and $10,001.

By 2 October 2018, Customer 59's annual losses had reached $503,653.

On 24 November 2018, Crown Melbourne recorded a machine payout to Customer 59 of $20,005.

By the end of 2018, Crown Melbourne recorded that Customer 59's annual losses had escalated exponentially to a total of $758,957.

EGM activity in 2019

By the end of 2019, Crown Melbourne recorded that Customer 59's annual losses had decreased compared to 2018, totalling $51,909.

1990. On and from 1 March 2016, on multiple occasions, enquiries by law enforcement agencies relating to Customer 59 raised red flags reflective of higher ML/TF risks for the provision of designated services to Customer 59 at Crown Melbourne.

Particulars

On 15 April 2016, 14 July 2016, 15 March 2017, and 20 April 2017, Crown Melbourne received law enforcement enquiries in respect of Customer 59.

From 12 July 2018, Crown Melbourne was aware that the law enforcement enquiries it was receiving concerned an investigation into Customer 59's involvement in suspected large-scale money laundering from proceeds of drug related activities.

Crown Melbourne received further law enforcement enquiries on 29 August 2018, 5 November 2018, 3 December 2018, and 4 December 2018.

1991. At no time did Crown Melbourne undertake appropriate risk-based customer due diligence with respect to Customer 59 with a view to identifying, mitigating and managing the ML/TF risks posed by the provision of designated services on and from 1 March 2016.

a. At no time did Crown Melbourne take appropriate steps to understand whether Customer 59's source of wealth/funds was legitimate.

b. At no time did Crown Melbourne take appropriate steps to identify or analyse the ML/TF risks of Customer 59's transactions or to consider whether they had a lawful purpose.

c. At no time did Crown Melbourne give appropriate consideration to whether large and high risk transactions should be processed.

d. On 14 November 2016, the POI Committee considered whether a business relationship with Customer 59 was within its ML/TF risk appetite, but determined that it would continue to conduct a business relationship with Customer 59 despite the high ML/TF risk that he posed.

e. On each occasion prior to November 2020 that senior management considered whether to continue the business relationship with Customer 59, senior management failed to give adequate consideration to whether the ML/TF risks posed by Customer 59 were within Crown Melbourne's risk appetite.

Particulars

Section 36(1)(a) of the Act.

The due diligence steps taken with respect to Customer 59 included:

Database searches

On 2 November 2016, Crown Melbourne performed a risk intelligence search on Customer 59, which reported that he had been charged with trafficking in methamphetamine and being sentenced to 19 months imprisonment in June 2014.

On 7 November 2018 and 28 January 2020, Crown Melbourne conducted further risk intelligence and media searches on Customer

59, which reported on Customer 59's convictions for drugs trafficking, including further charges in March 2019.

Senior management engagement

On 2 November 2016, the risk intelligence report was provided to Crown senior management, who determined to refer Customer 59 to the POI Committee. The CTRM rated Customer 59 high risk, placed an alert against Customer 59 in Crown Melbourne's SYCO database and gave the AUSTRAC CEO an SMR reporting the risk intelligence search findings.

On 14 November 2016, the POI Committee convened to discuss Customer 59. The POI Committee concluded that notwithstanding concerns regarding Customer 59's source of funds/source of wealth, there was too much of a delay from the time of charges to take action. The Committee decided not to issue a WOL. An alert was placed on Customer 59's account.

Between 15 March 2017 and 4 December 2018, Crown was aware of and responded to multiple law enforcement requests for information in relation to suspected large-scale money laundering from proceeds of drug related activities: see paragraph 1990.

On 29 August 2018, the Group General Manager – AML requested the CTRM and Compliance Manager to consider whether to file an SMR or refer Customer 59 to the POI Committee. An SMR was subsequently submitted on 29 August 2018.

On 28 January 2020, the AML Manager (Crown Melbourne) reviewed the law enforcement inquiries, media reports and SYCO records with respect to Customer 59 and concluded that Customer 59 should be referred to the POI Committee. The Manager (Compliance Reporting) noted that he would contact law enforcement to obtain further information about charges against Customer 59. No further steps were taken until October 2020.

On 22 October 2020, the Crown Melbourne CEO recommended that Customer 59 be referred to the POI Committee.

On 25 October 2020, the AML Manager (Crown Melbourne) recommended to the POI Committee that Customer 59 be issued with a WOL and excluded from Crown Melbourne. The AML Manager (Crown Melbourne) noted that Customer 59 was arrested in March 2019 for drug-related offences but not yet convicted, Crown had received 11 law enforcement inquiries and had assisted with police operations in relation to Customer 59 between 2015 and 2019.

On 23 November 2020, Crown Melbourne issued a WOL in respect of Customer 59.

Enhanced customer due diligence

1992. Having formed a suspicion for the purposes of s41 of the Act, Crown Melbourne gave the AUSTRAC CEO SMRs with respect to Customer 59 on:

a. 20 April 2016;

b. 20 July 2016;

c. 3 November 2016;

d. 11 September 2017;

e. 18 January 2018;

f. 5 June 2018;

g. 29 August 2018;

h. 2 October 2018; and

i. 9 November 2018.

Particulars

The SMRs reported on Customer 59's high annual losses and the large amounts of cash he was prepared to carry.

1993. On each occasion that Crown Melbourne formed a suspicion with respect to Customer 59 for the purposes of s41 of the Act, it was required to apply its ECDD program to Customer 59.

Particulars

Rule 15.9(3) of the Rules.

1994. Crown Melbourne did not carry out appropriate risk-based ECDD measures with respect to Customer 59 on each occasion that Crown Melbourne formed a suspicion with respect to Customer 59 for the purposes of s41 of the Act.

a. There are no records of ECDD being conducted following the lodgement of any SMRs by Crown Melbourne: see paragraphs 664 and 685.

b. Appropriate risk-based steps were not taken to obtain or analyse information about Customer 59's source of wealth/funds: see paragraph 667.

c. Appropriate risk-based steps were not taken to analyse and monitor Customer 59's transactions – both past and future – including to understand their economic purpose: see paragraphs 590 and 666.

d. On each occasion prior to November 2020 that senior management considered whether to continue the business relationship with Customer 59, senior management failed to give adequate consideration to whether the ML/TF risks posed by Customer 59 were within Crown Melbourne's risk appetite: see paragraph 668ff.

Particulars

Rules 15.9(3), 15.10(1)(c), (d), (2), (5) and (6) of the Rules.

See particulars to paragraph 1991.

1995. On and from 2 November 2016, Crown Melbourne rated Customer 59 high risk.

Particulars

Crown Melbourne rated Customer 59 high risk on 18 occasions between 2 November 2016 and 16 February 2021: see paragraph 1986.

1996. On each occasion that Crown Melbourne rated Customer 59 high risk, Crown Melbourne was required to apply its ECDD program to Customer 59.

Particulars

Rule 15.9(1) of the Rules.

See paragraph 661.

1997. Crown Melbourne did not carry out appropriate risk-based ECDD measures with respect to Customer 59 on each occasion that Crown Melbourne rated Customer 59 high risk.

Particulars

At no time did Crown Melbourne conduct ECDD following each occasion that it rated Customer 59 high risk, despite the higher ML/TF risks known to Crown Melbourne: see paragraph 1994.

See paragraphs 661, 666, 667 and 668.

1998. By reason of the matters pleaded from paragraphs 1981 to 1997, on and from 1 March 2016, Crown Melbourne:

a. did not monitor Customer 59 in relation to the provision of designated services, with a view to identifying, mitigating and managing the ML/TF risks reasonably faced; and

b. did not do so in accordance with rr 15.5 and 15.9 of the Rules.

1999. By reason of the matters pleaded at paragraph 1998, Crown Melbourne contravened s36(1) of the Act on and from 1 March 2016 to 23 November 2020 with respect to Customer 59.

Particulars

Section 36(1) of the Act is a civil penalty provision: s36(2) of the Act.

Customer 60

2000. Customer 60 was a customer of Crown Melbourne from 13 June 1994 to December 2019.

2001. From at least December 2006 to December 2019, Crown Melbourne provided Customer 60 with designated services within the meaning of table 1 and table 3, s6 of the Act.

Particulars

Between 2012 and 2015, Crown Melbourne recorded Customer 60's rated gaming activity as a cumulative turnover of $301,145 with a loss of $176,756.

On 10 December 2019, Crown Melbourne issued an indefinite WOL in respect of Customer 60 following his conviction for dishonesty causing a loss or risk to the Commonwealth between 1 October 2011 and 19 October 2014.

The ML/TF risks posed by Customer 60

2002. By 1 March 2016, higher ML/TF risks were indicated by the nature and purpose of Customer 60's business relationship with Crown Melbourne, the nature of the transactions he had been

conducting, together with the suspicions Crown Melbourne itself had formed with respect to Customer 60.

Particulars

Section 36(1)(a), (b) of the Act and Chapter 15 of the Rules.

By 1 March 2016, Crown Melbourne had given the AUSTRAC CEO one SMR in relation to Customer 60 on 20 May 2013. The SMR reported the suspicions relating to high losses.

The SMRs given to the AUSTRAC CEO in 2013 reported total losses of $167,956 over a 2 year period.

In 2012, Crown Melbourne recorded Customer 60's rated individual activity to be a turnover of $245,045 with a loss $151,746.

In 2013, Crown Melbourne recorded Customer 60's rated individual activity to be a turnover of $36,600 with a loss $16,210.

In 2014, Crown Melbourne recorded Customer 60's rated individual activity to be a turnover of $14,400 with a loss $5,600.

In 2015, Crown Melbourne recorded Customer 60's rated individual activity to be a turnover of $5,100 with a loss $3,200.

By 1 March 2016, there had been no due diligence steps taken with respect to Customer 60.

2003. As at 1 March 2016, Customer 60 should have been recognised by Crown Melbourne as a high risk customer for the reasons pleaded at paragraph 2002.

Particulars

Section 36(1)(a), (b) of the Act and Chapter 15 of the Rules.

2004. It was not until 11 July 2018 that Customer 60 was rated high risk by Crown Melbourne.

Particulars

On 20 May 2013, following submission of the first SMR in relation to Customer 60, Crown Melbourne assessed Customer 60 as moderate risk.

On 15 December 2017, Crown Melbourne assessed Customer 60 as significant risk.

On 11 July 2018, upon obtaining a risk intelligence search match on Customer 60, Crown Melbourne assessed Customer 60 as high risk.

This was despite Customer 60's high individual rated gaming activity and 2015 media reports identifying him to be one of three men charged as part of an investigation into alleged tax fraud and money laundering.

See paragraph 120.

2005. At all times on and from 1 March 2016, Customer 60 should have been recognised by Crown Melbourne as a high risk customer by reason of the matters pleaded at 2002, 2006, 2008, 2009 and 2011.

Particulars

Section 36(1)(a), (b) of the Act and Chapter 15 of the Rules.

2006. On and from 1 March 2016 designated services provided to Customer 60 posed higher ML/TF risks including because the provision of designated services to Customer 60 involved a combination of the following factors:

a. Customer 60 received high value gaming services (table 3, s6);

b. by 2019, Crown Melbourne recorded Customer 60's individual rated gaming activity to be a cumulative turnover of $1,279,185 with a cumulative loss of $424,191;

c. Customer 60 and persons associated with him carried and transacted in large and suspicious cash amounts;

d. in December 2017, Customer 60 was the subject of law enforcement inquiries;

e. by 12 July 2018, Crown Melbourne was aware that Customer 60 was associated with an individual that shared his last name, who had similarly high annual losses from rating gaming activity and was a person of interest in relation to a 2013 money laundering investigation. Customer 60 was also linked at that time to another individual who was a high profile OMCG identity;

f. by 11 July 2018, Crown Melbourne was aware:

i. of media reports from February 2015 that named Customer 60 as a person involved in alleged tax fraud and money laundering;

ii. that Customer 60 had been charged in February 2015 with fraud and money laundering offences, including financial structuring offences that were alleged to have taken place between October 2012 and November 2014; and

g. by reason of the matters set out at subparagraphs a. to f. above, there were real risks that Customer 60's source of wealth and source of funds were not legitimate.

Monitoring of Customer 60's transactions

2007. At no time did Crown Melbourne appropriately monitor Customer 60's transactions on a risk-basis.

Particulars

Section 36(1)(a), (b) of the Act and Rules 15.4 to 15.8 of the Rules.

Crown Melbourne did not apply appropriate risk-based transaction monitoring to designated services provided to Customer 60: see paragraphs 590ff and 629 to 642.

Ongoing customer due diligence

2008. During the following times, designated services provided to Customer 60 involved unusually large transactions and unusual patterns of transactions which had no apparent economic or visible lawful purpose:

Particulars

In 2016, Crown Melbourne recorded Customer 60's rated individual activity as escalating to a turnover of $258,500 with a loss of $104,491.

In 2017, Crown Melbourne recorded Customer 60's rated individual activity to be a turnover of $214,080 with a loss of $60,100

In December 2017, Customer 60 was the subject of law enforcement inquiries.

In 2018, Crown Melbourne recorded Customer 60's rated individual activity to be a turnover of $293,110 with a loss of $47,400

In 2019, Crown Melbourne recorded Customer 60's rated individual activity to be a turnover $212,350 with a loss $35,544

2009. Customer 60 was named in a number of media reports in February 2015 as one of three men charged as part of an investigation into alleged tax fraud, money laundering and illegal financial structuring. There was further media reports in March 2018 naming Customer 60 prior to his scheduled trial for those offences. Crown Melbourne does not have records of these media reports until 11 July 2018.

Particulars

Customer 60 was named in a number of media reports in February 2015 as one of three men charged as part of an investigation into alleged tax fraud, money laundering and illegal financial structuring. There was further media reports in March 2018 naming Customer 60 prior to his scheduled trial for those offences. Crown Melbourne does not have records of these media reports until 11 July 2018.

2010. At no time did Crown Melbourne undertake appropriate risk-based customer due diligence with respect to Customer 60 with a view to identifying, mitigating and managing the ML/TF risks posed by the provision of designated services on and from 1 March 2016.

a. At no time did Crown Melbourne take appropriate steps to understand whether Customer 60's source of wealth/funds was legitimate.

b. At no time did Crown Melbourne take appropriate steps to identify or analyse the ML/TF risks of Customer 60's transactions or to consider whether they had a lawful purpose.

c. At no time did Crown Melbourne give appropriate consideration to whether large and high risk transactions should be processed.

d. Prior to the decision to issue Customer 60 with a WOL in December 2019, there is no record of senior management considering whether continuing the business relationship with Customer 60 was within Crown Melbourne's ML/TF risk appetite in light of the ML/TF risks posed by Customer 60.

Particulars

Section 36(1)(a) of the Act.

The due diligence steps taken with respect to Customer 60 included:

- risk intelligence searches on 11 July 2018, which revealed that Customer 60 had been charged with fraud and money laundering offences in February 2015, and 12 November 2019; and
- an open source media report search on 12 November 2019.

None of these steps were proportionate to the ML/TF risks reasonably posed by Customer 60 on and from 1 March 2016.

On 10 December 2019, Crown Melbourne issued an indefinite WOL in respect of Customer 60 following his conviction for dishonesty causing a loss or risk to the Commonwealth between 1 October 2011 and 19 October 2014.

Enhanced customer due diligence

2011. Having formed a suspicion for the purposes of s41 of the Act, Crown Melbourne gave the AUSTRAC CEO SMRs with respect to Customer 60 on:

a. 31 May 2017; and

b. 11 July 2018.

Particulars

On 31 May 2017, Crown Melbourne submitted an SMR. The suspicion was based on Customer 60's annual losses from his rated gaming activity at Crown Melbourne.

On 11 July 2018, Crown Melbourne submitted an SMR based on a risk intelligence search match to Customer 60, which reported that in February 2015, Customer 60 was charged with tax fraud that was alleged to have occurred between October 2012 and November 2014, his annual losses, his association with another individual of the same surname with similarly high losses and the amounts of cash both patrons were willing to carry.

2012. On each occasion that Crown Melbourne formed a suspicion with respect to Customer 60 for the purposes of s41 of the Act, it was required to apply its ECDD program to Customer 60.

Particulars

Rule 15.9(3) of the Rules.

2013. Crown Melbourne did not carry out appropriate risk-based ECDD measures with respect to Customer 60 on each occasion that Crown Melbourne formed a suspicion with respect to Customer 60 for the purposes of s41 of the Act.

a. There are no records of ECDD being conducted following the lodgement of SMRs on 31 May 2017 and 11 July 2018: see paragraphs 664 and 685.

b. Appropriate risk-based steps were not taken to obtain or analyse information about Customer 60's source of wealth/funds: see paragraph 667.

c. Appropriate risk-based steps were not taken to analyse and monitor Customer 60's transactions – both past and future – including to understand their economic purpose: see paragraphs 590 and 666.

d. Prior to the decision to issue Customer 60 with a WOL in December 2019, there is no record of senior management considering whether continuing the business relationship with Customer 60 was within Crown Melbourne's ML/TF risk appetite in light of the ML/TF risks posed by Customer 60: see paragraph 668ff.

Particulars

Rules 15.9(3), 15.10(1)(c), (d), (2), (5) and (6) of the Rules.

See particulars to paragraph 2010.

2014. On and from 11 July 2018, Crown Melbourne rated Customer 60 high risk.

Particulars

Crown Melbourne rated Customer 60 high risk on five occasions after 11 July 2018: see paragraph 2004.

2015. When Crown Melbourne rated Customer 60 high risk, Crown Melbourne was required to apply its ECDD program to Customer 60.

Particulars

Rule 15.9(1) of the Rules.

See paragraph 661.

2016. Crown Melbourne did not carry out appropriate risk-based ECDD measures with respect to Customer 60 when Crown Melbourne rated Customer 60 high risk.

Particulars

Crown had identified high losses in the SMRs submitted in 2017 and 2018 in relation to Customer 60.

At no time did Crown Melbourne conduct ECDD following rating Customer 60 high risk, despite his being charged for fraud and money laundering offences in February 2015 and pleading guilty to those offences in September 2018. Those facts were widely reported in the media at the time and known to Crown Melbourne from 11 July 2018.

See paragraphs 661, 666, 667 and 668.

See also paragraph 2013.

2017. By reason of the matters pleaded from paragraphs 2000 to 2016, on and from 1 March 2016, Crown Melbourne:

a. did not monitor Customer 60 in relation to the provision of designated services, with a view to identifying, mitigating and managing the ML/TF risks reasonably faced; and

b. did not do so in accordance with rr 15.5 and 15.9 of the Rules.

2018. By reason of the matters pleaded at paragraph 2017, Crown Melbourne contravened s36(1) of the Act on and from 1 March 2016 to 10 December 2019 with respect to Customer 60.

Particulars

Section 36(1) of the Act is a civil penalty provision: s36(2) of the Act.

Failure to monitor customers for ML/TF typologies - structuring, cuckoo smurfing, chip cashing and quick chip turnover with minimal or no gaming

2019. From the date listed in column 2 until the date listed in column 3 of Confidential Schedule 1, Crown Melbourne or Crown Perth (as specified in column 4) provided a DAB account and/or safekeeping account to each of the customers listed in column 1 in Confidential Schedule 1.

2020. Within the period from the dates listed in column 2 to the date listed in column 3 of Confidential Schedule 1, Crown Melbourne or Crown Perth provided the customers listed in column 1 of Confidential Schedule 1 with designated services within the meaning of item 13 table 3, s6 of the Act with respect to these DAB accounts.

2021. Crown Melbourne or Crown Perth accepted or transferred funds for, or on behalf of, each of the customers listed in Confidential Schedule 1 through a Crown Patron account, including the Southbank/Riverbank accounts.

a. These funds were deposited into, or transferred from, DAB accounts provided to each of these customers.

b. Transactions on DAB accounts were designated services provided by Crown Melbourne or Crown Perth to each customer within the meaning of item 13 table 3, s6 of the Act.

c. These transactions also involved item 31 and/or 32, table 1, s6 designated services and facilitated other table 3, s6 designated services.

2022. Crown Melbourne or Crown Perth did not apply appropriate risk-based transaction monitoring to the transactions of customers on DAB accounts at any time.

Particulars

See paragraph 593.

2023. At no time, did Crown Melbourne or Crown Perth apply appropriate risk-based transaction monitoring to DAB accounts to detect transactions potentially indicative of:

a. structuring;

b. cuckoo smurfing;

c. smurfing;

d. chip or CVI cashing with minimal or no gaming activity; and/or

e. quick turnover of chips or CVIs with minimal or no gaming activity.

Particulars

Paragraph 593.

2024. Transactions conducted on the DAB Accounts by the customers in Confidential Schedule 1 between the dates listed in column 2 and column 3 of Confidential Schedule 1 had the indicia of one or more of these typologies.

2025. By failing to apply appropriate risk-based transaction monitoring to DAB Accounts, Crown Melbourne or Crown Perth failed to monitor each of the 447 customers listed in Confidential Schedule 1 with a view to identifying, mitigating and managing the ML/TF risks it reasonably faced in relation to the provision of designated services.

2026. By reason of the matters pleaded at paragraphs 2019 to 2025, Crown Melbourne or Crown Perth did not monitor each of the 447 customers listed in Confidential Schedule 1 in relation to the provision of designated services, with a view to identifying, mitigating and managing the ML/TF risks it reasonably faced, and did not do so in accordance with the Rules.

2027. By reason of the matters pleaded at paragraph 2026, Crown Melbourne or Crown Perth contravened s 36(1) of the Act on 464 occasions in relation to the customers listed in column 1 of Confidential Schedule 1 from the date listed in column 2 until the date listed in column 3 of Confidential Schedule 1.

Particulars

Section 36(1) of the Act is a civil penalty provision: s36(2) of the Act.

And the Applicant claims the relief specified in the accompanying Application.

Date: 1 March 2022

.....

Sonja Marsic
AGS Lawyer
for and on behalf of the Australian Government Solicitor
Lawyer for the Applicant

This pleading was prepared by Sonja Marsic, lawyer.

CERTIFICATE OF LAWYER

I, Sonja Marsic, certify to the Court that, in relation to the statement of claim filed on behalf of the Applicant, the factual and legal material available to me at present provides a proper basis for each allegation in the pleading.

Date: 1 March 2022

.....

Sonja Marsic
AGS Lawyer
for and on behalf of the Australian Government Solicitor
Lawyer for the Applicant

Schedule 1 (confidential)

This schedule is confidential. This page has been intentionally left blank.

Schedule 2 (confidential)

This schedule is confidential. This page has been intentionally left blank.

Schedule 3

Suspicious Matter Reports given to the AUSTRAC CEO in respect of:

3.1. Customer 1

3.2. Customer 2

3.3. Customer 3

3.4. Customer 4

3.5. Customer 5

3.6. Customer 6

3.7. Customer 20

3.8. Customer 22

SCHEDULE 3.1 (CUSTOMER 1)

No	SMR date	Crown property
1.	1 March 2016	Crown Melbourne
2.	1 March 2016	Crown Melbourne
3.	1 April 2016	Crown Melbourne
4.	2 May 2016	Crown Melbourne
5.	31 May 2016	Crown Melbourne
6.	23 June 2016	Crown Melbourne
7.	5 July 2016	Crown Melbourne
8.	18 July 2016	Crown Melbourne
9.	19 July 2016	Crown Melbourne
10.	1 August 2016	Crown Melbourne
11.	1 September 2016	Crown Melbourne
12.	3 October 2016	Crown Melbourne
13.	6 October 2016	Crown Melbourne
14.	24 October 2016	Crown Melbourne
15.	27 October 2016	Crown Melbourne
16.	2 November 2016	Crown Melbourne
17.	2 November 2016	Crown Melbourne
18.	7 November 2016	Crown Melbourne
19.	10 November 2016	Crown Melbourne
20.	23 November 2016	Crown Melbourne

21.	1 December 2016	Crown Melbourne
22.	1 December 2016	Crown Melbourne
23.	12 December 2016	Crown Melbourne
24.	15 December 2016	Crown Melbourne
25.	3 January 2017	Crown Melbourne
26.	3 January 2017	Crown Melbourne
27.	2 February 2017	Crown Melbourne
28.	27 February 2017	Crown Melbourne
29.	1 March 2017	Crown Melbourne
30.	17 March 2017	Crown Melbourne
31.	24 March 2017	Crown Melbourne
32.	3 April 2017	Crown Melbourne
33.	27 April 2017	Crown Melbourne
34.	1 May 2017	Crown Melbourne
35.	12 May 2017	Crown Melbourne
36.	31 May 2017	Crown Melbourne
37.	22 June 2017	Crown Melbourne
38.	2 August 2017	Crown Melbourne
39.	31 August 2017	Crown Melbourne
40.	1 September 2017	Crown Melbourne
41.	21 September 2017	Crown Melbourne
42.	2 October 2017	Crown Melbourne
43.	6 October 2017	Crown Melbourne
44.	9 October 2017	Crown Melbourne
45.	16 October 2017	Crown Melbourne
46.	23 October 2017	Crown Melbourne
47.	2 November 2017	Crown Melbourne
48.	2 November 2017	Crown Melbourne
49.	17 November 2017	Crown Melbourne
50.	24 November 2017	Crown Melbourne
51.	27 November 2017	Crown Melbourne
52.	27 November 2017	Crown Melbourne
53.	29 November 2017	Crown Melbourne
54.	29 November 2017	Crown Melbourne
55.	30 November 2017	Crown Melbourne

56.	30 November 2017	Crown Melbourne
57.	1 December 2017	Crown Melbourne
58.	1 December 2017	Crown Melbourne
59.	1 December 2017	Crown Melbourne
60.	4 December 2017	Crown Melbourne
61.	4 December 2017	Crown Melbourne
62.	4 December 2017	Crown Melbourne
63.	6 December 2017	Crown Melbourne
64.	8 December 2017	Crown Melbourne
65.	13 December 2017	Crown Melbourne
66.	15 December 2017	Crown Melbourne
67.	18 December 2017	Crown Melbourne
68.	19 December 2017	Crown Melbourne
69.	22 December 2017	Crown Melbourne
70.	22 December 2017	Crown Melbourne
71.	22 December 2017	Crown Melbourne
72.	28 December 2017	Crown Melbourne
73.	29 December 2017	Crown Melbourne
74.	2 January 2018	Crown Melbourne
75.	2 January 2018	Crown Melbourne
76.	2 January 2018	Crown Melbourne
77.	2 January 2018	Crown Melbourne
78.	2 January 2018	Crown Melbourne
79.	2 January 2018	Crown Melbourne
80.	2 January 2018	Crown Melbourne
81.	2 January 2018	Crown Melbourne
82.	2 January 2018	Crown Melbourne
83.	2 January 2018	Crown Melbourne
84.	2 January 2018	Crown Melbourne
85.	2 January 2018	Crown Melbourne
86.	2 January 2018	Crown Melbourne
87.	3 January 2018	Crown Melbourne
88.	3 January 2018	Crown Melbourne
89.	8 January 2018	Crown Melbourne
90.	9 January 2018	Crown Melbourne

91.	9 January 2018	Crown Melbourne
92.	11 January 2018	Crown Melbourne
93.	12 January 2018	Crown Melbourne
94.	15 January 2018	Crown Melbourne
95.	15 January 2018	Crown Melbourne
96.	16 January 2018	Crown Melbourne
97.	17 January 2018	Crown Melbourne
98.	23 January 2018	Crown Melbourne
99.	25 January 2018	Crown Melbourne
100.	29 January 2018	Crown Melbourne
101.	31 January 2018	Crown Melbourne
102.	1 February 2018	Crown Melbourne
103.	1 February 2018	Crown Melbourne
104.	9 February 2018	Crown Melbourne
105.	14 February 2018	Crown Melbourne
106.	15 February 2018	Crown Melbourne
107.	16 February 2018	Crown Melbourne
108.	20 February 2018	Crown Melbourne
109.	21 February 2018	Crown Melbourne
110.	26 February 2018	Crown Melbourne
111.	26 February 2018	Crown Melbourne
112.	27 February 2018	Crown Melbourne
113.	27 February 2018	Crown Melbourne
114.	1 March 2018	Crown Melbourne
115.	1 March 2018	Crown Melbourne
116.	8 March 2018	Crown Melbourne
117.	9 March 2018	Crown Melbourne
118.	15 March 2018	Crown Melbourne
119.	16 March 2018	Crown Melbourne
120.	16 March 2018	Crown Melbourne
121.	19 March 2018	Crown Melbourne
122.	19 March 2018	Crown Melbourne
123.	21 March 2018	Crown Melbourne
124.	21 March 2018	Crown Melbourne
125.	23 March 2018	Crown Melbourne

126.	27 March 2018	Crown Melbourne
127.	28 March 2018	Crown Melbourne
128.	29 March 2018	Crown Melbourne
129.	3 April 2018	Crown Melbourne
130.	3 April 2018	Crown Melbourne
131.	3 April 2018	Crown Melbourne
132.	6 April 2018	Crown Melbourne
133.	16 April 2018	Crown Melbourne
134.	16 April 2018	Crown Melbourne
135.	16 April 2018	Crown Melbourne
136.	17 April 2018	Crown Melbourne
137.	19 April 2018	Crown Melbourne
138.	23 April 2018	Crown Melbourne
139.	1 May 2018	Crown Melbourne
140.	1 May 2018	Crown Melbourne
141.	4 May 2018	Crown Melbourne
142.	9 May 2018	Crown Melbourne
143.	1 June 2018	Crown Melbourne
144.	6 June 2018	Crown Melbourne
145.	18 June 2018	Crown Melbourne
146.	2 July 2018	Crown Melbourne
147.	2 July 2018	Crown Melbourne
148.	6 July 2018	Crown Melbourne
149.	19 July 2018	Crown Melbourne
150.	23 July 2018	Crown Melbourne
151.	1 August 2018	Crown Melbourne
152.	3 August 2018	Crown Melbourne
153.	3 August 2018	Crown Melbourne
154.	6 August 2018	Crown Melbourne
155.	14 August 2018	Crown Melbourne
156.	15 August 2018	Crown Melbourne
157.	22 August 2018	Crown Melbourne
158.	23 August 2018	Crown Melbourne
159.	27 August 2018	Crown Melbourne
160.	30 August 2018	Crown Melbourne

161.	5 September 2018	Crown Melbourne
162.	10 September 2018	Crown Melbourne
163.	20 September 2018	Crown Melbourne
164.	27 September 2018	Crown Melbourne
165.	10 October 2018	Crown Melbourne
166.	23 October 2018	Crown Melbourne
167.	7 November 2018	Crown Melbourne
168.	12 November 2018	Crown Melbourne
169.	26 November 2018	Crown Melbourne
170.	30 November 2018	Crown Melbourne
171.	7 December 2018	Crown Melbourne
172.	17 December 2018	Crown Melbourne
173.	21 December 2018	Crown Melbourne
174.	10 January 2019	Crown Melbourne
175.	15 January 2019	Crown Melbourne
176.	21 February 2019	Crown Melbourne
177.	6 March 2019	Crown Melbourne
178.	14 March 2019	Crown Melbourne
179.	19 March 2019	Crown Melbourne
180.	20 March 2019	Crown Melbourne
181.	22 March 2019	Crown Melbourne
182.	28 March 2019	Crown Melbourne
183.	4 April 2019	Crown Melbourne
184.	18 April 2019	Crown Melbourne
185.	26 April 2019	Crown Melbourne
186.	7 May 2019	Crown Melbourne
187.	10 May 2019	Crown Melbourne
188.	16 May 2019	Crown Melbourne
189.	22 May 2019	Crown Melbourne
190.	24 May 2019	Crown Melbourne
191.	28 May 2019	Crown Melbourne
192.	29 May 2019	Crown Melbourne
193.	6 June 2019	Crown Melbourne
194.	13 June 2019	Crown Melbourne
195.	5 July 2019	Crown Melbourne

196.	15 July 2019	Crown Melbourne
197.	18 July 2019	Crown Melbourne
198.	18 July 2019	Crown Melbourne
199.	25 July 2019	Crown Melbourne
200.	31 July 2019	Crown Melbourne
201.	23 September 2019	Crown Melbourne
202.	13 November 2019	Crown Melbourne
203.	21 November 2019	Crown Melbourne
204.	16 December 2019	Crown Melbourne
205.	27 December 2019	Crown Melbourne
206.	1 January 2020	Crown Melbourne
207.	2 January 2020	Crown Melbourne
208.	3 January 2020	Crown Melbourne
209.	21 February 2020	Crown Melbourne
210.	27 November 2020	Crown Melbourne
211.	23 February 2018	Crown Perth
212.	9 March 2018	Crown Perth
213.	23 November 2018	Crown Perth
214.	24 July 2019	Crown Perth
215.	24 March 2020	Crown Perth

SCHEDULE 3.2 (CUSTOMER 2)

No	SMR date	Crown property
1.	6 April 2016	Crown Melbourne
2.	27 April 2016	Crown Melbourne
3.	6 May 2016	Crown Melbourne
4.	17 May 2016	Crown Melbourne
5.	23 May 2016	Crown Melbourne
6.	31 May 2016	Crown Melbourne
7.	1 June 2016	Crown Melbourne
8.	22 June 2016	Crown Melbourne
9.	6 July 2016	Crown Melbourne
10.	1 August 2016	Crown Melbourne
11.	11 August 2016	Crown Melbourne
12.	7 October 2016	Crown Melbourne
13.	19 October 2016	Crown Melbourne
14.	11 November 2016	Crown Melbourne
15.	1 December 2016	Crown Melbourne
16.	16 December 2016	Crown Melbourne
17.	24 January 2017	Crown Melbourne
18.	1 March 2017	Crown Melbourne
19.	23 March 2017	Crown Melbourne
20.	11 April 2017	Crown Melbourne
21.	27 April 2017	Crown Melbourne
22.	12 May 2017	Crown Melbourne
23.	15 June 2017	Crown Melbourne
24.	19 June 2017	Crown Melbourne
25.	9 August 2017	Crown Melbourne
26.	21 August 2017	Crown Melbourne
27.	22 August 2017	Crown Melbourne
28.	4 September 2017	Crown Melbourne
29.	11 September 2017	Crown Melbourne
30.	11 September 2017	Crown Melbourne
31.	13 September 2017	Crown Melbourne
32.	10 October 2017	Crown Melbourne
33.	1 November 2017	Crown Melbourne

34.	6 November 2017	Crown Melbourne
35.	8 November 2017	Crown Melbourne
36.	10 November 2017	Crown Melbourne
37.	14 November 2017	Crown Melbourne
38.	30 November 2017	Crown Melbourne
39.	4 December 2017	Crown Melbourne
40.	6 December 2017	Crown Melbourne
41.	12 December 2017	Crown Melbourne
42.	18 December 2017	Crown Melbourne
43.	2 January 2018	Crown Melbourne
44.	3 January 2018	Crown Melbourne
45.	9 January 2018	Crown Melbourne
46.	9 January 2018	Crown Melbourne
47.	10 January 2018	Crown Melbourne
48.	11 January 2018	Crown Melbourne
49.	12 January 2018	Crown Melbourne
50.	15 January 2018	Crown Melbourne
51.	17 January 2018	Crown Melbourne
52.	29 January 2018	Crown Melbourne
53.	2 February 2018	Crown Melbourne
54.	9 February 2018	Crown Melbourne
55.	12 February 2018	Crown Melbourne
56.	13 February 2018	Crown Melbourne
57.	15 February 2018	Crown Melbourne
58.	19 February 2018	Crown Melbourne
59.	1 March 2018	Crown Melbourne
60.	2 March 2018	Crown Melbourne
61.	6 March 2018	Crown Melbourne
62.	22 March 2018	Crown Melbourne
63.	29 March 2018	Crown Melbourne
64.	4 April 2018	Crown Melbourne
65.	11 April 2018	Crown Melbourne
66.	12 April 2018	Crown Melbourne
67.	18 April 2018	Crown Melbourne
68.	27 April 2018	Crown Melbourne

69.	10 May 2018	Crown Melbourne
70.	10 May 2018	Crown Melbourne
71.	24 May 2018	Crown Melbourne
72.	1 June 2018	Crown Melbourne
73.	27 June 2018	Crown Melbourne
74.	4 July 2018	Crown Melbourne
75.	6 July 2018	Crown Melbourne
76.	9 July 2018	Crown Melbourne
77.	17 July 2018	Crown Melbourne
78.	19 July 2018	Crown Melbourne
79.	20 July 2018	Crown Melbourne
80.	23 July 2018	Crown Melbourne
81.	24 July 2018	Crown Melbourne
82.	25 July 2018	Crown Melbourne
83.	27 July 2018	Crown Melbourne
84.	30 July 2018	Crown Melbourne
85.	2 August 2018	Crown Melbourne
86.	3 August 2018	Crown Melbourne
87.	3 August 2018	Crown Melbourne
88.	6 August 2018	Crown Melbourne
89.	10 August 2018	Crown Melbourne
90.	13 August 2018	Crown Melbourne
91.	15 August 2018	Crown Melbourne
92.	20 August 2018	Crown Melbourne
93.	22 August 2018	Crown Melbourne
94.	23 August 2018	Crown Melbourne
95.	24 August 2018	Crown Melbourne
96.	27 August 2018	Crown Melbourne
97.	27 August 2018	Crown Melbourne
98.	28 August 2018	Crown Melbourne
99.	31 August 2018	Crown Melbourne
100.	3 September 2018	Crown Melbourne
101.	4 September 2018	Crown Melbourne
102.	5 September 2018	Crown Melbourne
103.	20 September 2018	Crown Melbourne

104.	24 September 2018	Crown Melbourne
105.	26 September 2018	Crown Melbourne
106.	1 October 2018	Crown Melbourne
107.	3 October 2018	Crown Melbourne
108.	10 October 2018	Crown Melbourne
109.	11 October 2018	Crown Melbourne
110.	12 October 2018	Crown Melbourne
111.	15 October 2018	Crown Melbourne
112.	16 October 2018	Crown Melbourne
113.	17 October 2018	Crown Melbourne
114.	18 October 2018	Crown Melbourne
115.	19 October 2018	Crown Melbourne
116.	22 October 2018	Crown Melbourne
117.	24 October 2018	Crown Melbourne
118.	26 October 2018	Crown Melbourne
119.	31 October 2018	Crown Melbourne
120.	1 November 2018	Crown Melbourne
121.	2 November 2018	Crown Melbourne
122.	7 November 2018	Crown Melbourne
123.	9 November 2018	Crown Melbourne
124.	12 November 2018	Crown Melbourne
125.	14 November 2018	Crown Melbourne
126.	16 November 2018	Crown Melbourne
127.	19 November 2018	Crown Melbourne
128.	20 November 2018	Crown Melbourne
129.	22 November 2018	Crown Melbourne
130.	26 November 2018	Crown Melbourne
131.	30 November 2018	Crown Melbourne
132.	3 December 2018	Crown Melbourne
133.	5 December 2018	Crown Melbourne
134.	6 December 2018	Crown Melbourne
135.	11 December 2018	Crown Melbourne
136.	12 December 2018	Crown Melbourne
137.	13 December 2018	Crown Melbourne
138.	18 December 2018	Crown Melbourne

139.	19 December 2018	Crown Melbourne
140.	20 December 2018	Crown Melbourne
141.	21 December 2018	Crown Melbourne
142.	24 December 2018	Crown Melbourne
143.	27 December 2018	Crown Melbourne
144.	31 December 2018	Crown Melbourne
145.	3 January 2019	Crown Melbourne
146.	7 January 2019	Crown Melbourne
147.	8 January 2019	Crown Melbourne
148.	9 January 2019	Crown Melbourne
149.	11 January 2019	Crown Melbourne
150.	15 January 2019	Crown Melbourne
151.	16 January 2019	Crown Melbourne
152.	22 January 2019	Crown Melbourne
153.	23 January 2019	Crown Melbourne
154.	30 January 2019	Crown Melbourne
155.	4 February 2019	Crown Melbourne
156.	5 February 2019	Crown Melbourne
157.	5 February 2019	Crown Melbourne
158.	11 February 2019	Crown Melbourne
159.	12 February 2019	Crown Melbourne
160.	13 February 2019	Crown Melbourne
161.	18 February 2019	Crown Melbourne
162.	19 February 2019	Crown Melbourne
163.	22 February 2019	Crown Melbourne
164.	25 February 2019	Crown Melbourne
165.	1 March 2019	Crown Melbourne
166.	4 March 2019	Crown Melbourne
167.	19 March 2019	Crown Melbourne
168.	19 March 2019	Crown Melbourne
169.	1 April 2019	Crown Melbourne
170.	3 April 2019	Crown Melbourne
171.	4 April 2019	Crown Melbourne
172.	5 April 2019	Crown Melbourne
173.	9 April 2019	Crown Melbourne

174.	10 April 2019	Crown Melbourne
175.	15 April 2019	Crown Melbourne
176.	17 April 2019	Crown Melbourne
177.	18 April 2019	Crown Melbourne
178.	24 April 2019	Crown Melbourne
179.	26 April 2019	Crown Melbourne
180.	29 April 2019	Crown Melbourne
181.	1 May 2019	Crown Melbourne
182.	2 May 2019	Crown Melbourne
183.	20 May 2019	Crown Melbourne
184.	3 June 2019	Crown Melbourne
185.	4 June 2019	Crown Melbourne
186.	6 June 2019	Crown Melbourne
187.	12 June 2019	Crown Melbourne
188.	20 June 2019	Crown Melbourne
189.	27 June 2019	Crown Melbourne
190.	2 July 2019	Crown Melbourne
191.	3 July 2019	Crown Melbourne
192.	8 July 2019	Crown Melbourne
193.	22 July 2019	Crown Melbourne
194.	24 July 2019	Crown Melbourne
195.	29 July 2019	Crown Melbourne
196.	31 July 2019	Crown Melbourne
197.	31 July 2019	Crown Melbourne
198.	1 August 2019	Crown Melbourne
199.	2 August 2019	Crown Melbourne
200.	5 August 2019	Crown Melbourne
201.	7 August 2019	Crown Melbourne
202.	8 August 2019	Crown Melbourne
203.	9 August 2019	Crown Melbourne
204.	12 August 2019	Crown Melbourne
205.	14 August 2019	Crown Melbourne
206.	19 August 2019	Crown Melbourne
207.	21 August 2019	Crown Melbourne
208.	11 September 2019	Crown Melbourne

209.	12 September 2019	Crown Melbourne
210.	7 October 2019	Crown Melbourne
211.	11 October 2019	Crown Melbourne
212.	16 October 2019	Crown Melbourne
213.	22 October 2019	Crown Melbourne
214.	1 November 2019	Crown Melbourne
215.	6 November 2019	Crown Melbourne
216.	8 November 2019	Crown Melbourne
217.	15 November 2019	Crown Melbourne
218.	18 November 2019	Crown Melbourne
219.	4 December 2019	Crown Melbourne
220.	9 December 2019	Crown Melbourne
221.	16 December 2019	Crown Melbourne
222.	19 December 2019	Crown Melbourne
223.	20 December 2019	Crown Melbourne
224.	23 December 2019	Crown Melbourne
225.	1 January 2020	Crown Melbourne
226.	9 January 2020	Crown Melbourne
227.	11 March 2020	Crown Melbourne
228.	12 March 2020	Crown Melbourne
229.	13 March 2020	Crown Melbourne
230.	16 March 2020	Crown Melbourne
231.	17 March 2020	Crown Melbourne
232.	18 March 2020	Crown Melbourne
233.	18 March 2020	Crown Melbourne
234.	20 March 2020	Crown Melbourne
235.	22 November 2016	Crown Perth

SCHEDULE 3.3 (CUSTOMER 3)

No	SMR date	Crown property
1.	13 October 2016	Crown Melbourne
2.	8 March 2017	Crown Melbourne
3.	5 April 2017	Crown Melbourne
4.	2 May 2017	Crown Melbourne
5.	8 May 2017	Crown Melbourne
6.	13 June 2017	Crown Melbourne
7.	16 June 2017	Crown Melbourne
8.	23 June 2017	Crown Melbourne
9.	3 August 2017	Crown Melbourne
10.	14 August 2017	Crown Melbourne
11.	18 August 2017	Crown Melbourne
12.	22 August 2017	Crown Melbourne
13.	22 September 2017	Crown Melbourne
14.	28 September 2017	Crown Melbourne
15.	17 October 2017	Crown Melbourne
16.	18 October 2017	Crown Melbourne
17.	25 October 2017	Crown Melbourne
18.	28 November 2017	Crown Melbourne
19.	8 December 2017	Crown Melbourne
20.	29 December 2017	Crown Melbourne
21.	19 January 2018	Crown Melbourne
22.	19 February 2018	Crown Melbourne
23.	22 February 2018	Crown Melbourne
24.	28 February 2018	Crown Melbourne
25.	1 March 2018	Crown Melbourne
26.	5 March 2018	Crown Melbourne
27.	5 March 2018	Crown Melbourne
28.	7 March 2018	Crown Melbourne
29.	13 March 2018	Crown Melbourne
30.	28 March 2018	Crown Melbourne
31.	3 April 2018	Crown Melbourne
32.	3 April 2018	Crown Melbourne
33.	3 April 2018	Crown Melbourne

34.	16 April 2018	Crown Melbourne
35.	1 May 2018	Crown Melbourne
36.	1 May 2018	Crown Melbourne
37.	4 May 2018	Crown Melbourne
38.	17 May 2018	Crown Melbourne
39.	22 May 2018	Crown Melbourne
40.	4 June 2018	Crown Melbourne
41.	27 July 2018	Crown Melbourne
42.	3 August 2018	Crown Melbourne
43.	17 August 2018	Crown Melbourne
44.	20 August 2018	Crown Melbourne
45.	21 September 2018	Crown Melbourne
46.	30 October 2018	Crown Melbourne
47.	14 November 2018	Crown Melbourne
48.	15 November 2018	Crown Melbourne
49.	16 November 2018	Crown Melbourne
50.	19 November 2018	Crown Melbourne
51.	6 February 2019	Crown Melbourne
52.	13 February 2019	Crown Melbourne
53.	6 March 2019	Crown Melbourne
54.	13 March 2019	Crown Melbourne
55.	25 March 2019	Crown Melbourne
56.	10 April 2019	Crown Melbourne
57.	29 April 2019	Crown Melbourne
58.	12 June 2019	Crown Melbourne
59.	13 June 2019	Crown Melbourne
60.	14 June 2019	Crown Melbourne
61.	2 July 2019	Crown Melbourne
62.	3 July 2019	Crown Melbourne
63.	4 July 2019	Crown Melbourne
64.	24 July 2019	Crown Melbourne
65.	26 July 2019	Crown Melbourne
66.	30 July 2019	Crown Melbourne
67.	20 August 2019	Crown Melbourne
68.	3 October 2019	Crown Melbourne

69.	8 November 2019	Crown Melbourne
70.	13 November 2019	Crown Melbourne
71.	26 November 2019	Crown Melbourne
72.	3 December 2019	Crown Melbourne
73.	11 December 2019	Crown Melbourne
74.	23 December 2019	Crown Melbourne
75.	30 December 2019	Crown Melbourne
76.	9 January 2020	Crown Melbourne
77.	17 January 2020	Crown Melbourne
78.	7 February 2020	Crown Melbourne
79.	2 March 2020	Crown Melbourne
80.	5 March 2020	Crown Melbourne

SCHEDULE 3.4 (CUSTOMER 4)

Schedule 3.4.1 (Customer 4 pre-1 March 2016)

No	SMR date	Crown property
1.	3 May 2010	Crown Melbourne
2.	8 December 2010	Crown Melbourne
3.	11 February 2011	Crown Melbourne
4.	21 March 2011	Crown Melbourne
5.	12 July 2011	Crown Melbourne
6.	17 October 2011	Crown Melbourne
7.	13 February 2012	Crown Melbourne
8.	27 March 2012	Crown Melbourne
9.	27 April 2012	Crown Melbourne
10.	2 May 2012	Crown Melbourne
11.	3 January 2013	Crown Melbourne
12.	1 March 2013	Crown Melbourne
13.	8 March 2013	Crown Melbourne
14.	9 April 2013	Crown Melbourne
15.	19 April 2013	Crown Melbourne
16.	24 April 2013	Crown Melbourne
17.	16 May 2013	Crown Melbourne
18.	5 June 2013	Crown Melbourne
19.	6 June 2013	Crown Melbourne
20.	19 June 2013	Crown Melbourne
21.	26 June 2013	Crown Melbourne
22.	26 July 2013	Crown Melbourne
23.	13 August 2013	Crown Melbourne
24.	28 August 2013	Crown Melbourne
25.	6 September 2013	Crown Melbourne
26.	11 September 2013	Crown Melbourne
27.	24 September 2013	Crown Melbourne
28.	30 September 2013	Crown Melbourne
29.	28 October 2013	Crown Melbourne
30.	19 November 2013	Crown Melbourne
31.	16 December 2013	Crown Melbourne

32.	31 December 2013	Crown Melbourne
33.	28 January 2014	Crown Melbourne
34.	24 March 2014	Crown Melbourne
35.	27 March 2014	Crown Melbourne
36.	7 April 2014	Crown Melbourne
37.	14 April 2014	Crown Melbourne
38.	5 May 2014	Crown Melbourne
39.	9 May 2014	Crown Melbourne
40.	19 June 2014	Crown Melbourne
41.	24 June 2014	Crown Melbourne
42.	17 July 2014	Crown Melbourne
43.	21 July 2014	Crown Melbourne
44.	4 August 2014	Crown Melbourne
45.	22 August 2014	Crown Melbourne
46.	1 September 2014	Crown Melbourne
47.	5 September 2014	Crown Melbourne
48.	6 October 2014	Crown Melbourne
49.	29 October 2014	Crown Melbourne
50.	5 January 2015	Crown Melbourne
51.	19 January 2015	Crown Melbourne
52.	4 February 2015	Crown Melbourne
53.	17 February 2015	Crown Melbourne
54.	19 February 2015	Crown Melbourne
55.	3 March 2015	Crown Melbourne
56.	10 March 2015	Crown Melbourne
57.	25 March 2015	Crown Melbourne
58.	27 May 2015	Crown Melbourne
59.	28 May 2015	Crown Melbourne
60.	15 July 2015	Crown Melbourne
61.	22 July 2015	Crown Melbourne
62.	29 July 2015	Crown Melbourne
63.	29 July 2015	Crown Melbourne
64.	10 August 2015	Crown Melbourne
65.	12 August 2015	Crown Melbourne
66.	19 August 2015	Crown Melbourne

67.	11 September 2015	Crown Melbourne
68.	16 September 2015	Crown Melbourne
69.	30 September 2015	Crown Melbourne
70.	30 September 2015	Crown Melbourne
71.	6 October 2015	Crown Melbourne
72.	7 October 2015	Crown Melbourne
73.	19 October 2015	Crown Melbourne
74.	22 December 2015	Crown Melbourne
75.	18 January 2016	Crown Melbourne
76.	21 January 2016	Crown Melbourne
77.	19 February 2016	Crown Melbourne
78.	29 February 2016	Crown Melbourne
79.	29 February 2016	Crown Melbourne

Schedule 3.4.2 (Customer 4 post-1 March 2016)

No	**SMR date**	**Crown property**
80.	24 March 2016	Crown Melbourne
81.	4 April 2016	Crown Melbourne
82.	5 May 2016	Crown Melbourne
83.	20 May 2016	Crown Melbourne
84.	6 June 2016	Crown Melbourne
85.	27 June 2016	Crown Perth
86.	5 July 2016	Crown Melbourne
87.	6 July 2016	Crown Melbourne
88.	14 July 2016	Crown Perth
89.	1 August 2016	Crown Melbourne
90.	3 August 2016	Crown Melbourne
91.	26 August 2016	Crown Melbourne
92.	1 September 2016	Crown Melbourne
93.	2 September 2016	Crown Melbourne
94.	19 September 2016	Crown Melbourne
95.	6 October 2016	Crown Melbourne
96.	4 January 2017	Crown Melbourne
97.	5 January 2017	Crown Melbourne

98.	19 January 2017	Crown Melbourne
99.	30 January 2017	Crown Melbourne
100.	28 February 2017	Crown Melbourne
101.	28 February 2017	Crown Melbourne
102.	14 March 2017	Crown Melbourne
103.	29 March 2017	Crown Melbourne
104.	26 April 2017	Crown Melbourne
105.	28 April 2017	Crown Melbourne
106.	4 May 2017	Crown Melbourne
107.	25 May 2017	Crown Melbourne
108.	26 June 2017	Crown Melbourne
109.	3 July 2017	Crown Melbourne
110.	7 August 2017	Crown Melbourne
111.	5 October 2017	Crown Melbourne
112.	6 October 2017	Crown Melbourne
113.	9 October 2017	Crown Melbourne
114.	16 October 2017	Crown Melbourne
115.	31 October 2017	Crown Melbourne
116.	31 October 2017	Crown Melbourne
117.	6 December 2017	Crown Melbourne
118.	20 December 2017	Crown Melbourne
119.	3 January 2018	Crown Melbourne
120.	29 January 2018	Crown Melbourne
121.	12 February 2018	Crown Melbourne
122.	20 February 2018	Crown Melbourne
123.	1 March 2018	Crown Melbourne
124.	1 March 2018	Crown Melbourne
125.	2 March 2018	Crown Melbourne
126.	15 March 2018	Crown Melbourne
127.	16 April 2018	Crown Melbourne
128.	22 May 2018	Crown Melbourne
129.	29 May 2018	Crown Melbourne
130.	26 June 2018	Crown Melbourne
131.	18 July 2018	Crown Melbourne
132.	27 July 2018	Crown Melbourne

133.	1 August 2018	Crown Melbourne
134.	2 August 2018	Crown Melbourne
135.	3 August 2018	Crown Melbourne
136.	7 August 2018	Crown Melbourne
137.	16 August 2018	Crown Melbourne
138.	17 August 2018	Crown Melbourne
139.	20 August 2018	Crown Melbourne
140.	23 August 2018	Crown Melbourne
141.	20 September 2018	Crown Melbourne
142.	1 October 2018	Crown Melbourne
143.	24 October 2018	Crown Melbourne
144.	26 October 2018	Crown Melbourne
145.	31 October 2018	Crown Melbourne
146.	22 November 2018	Crown Melbourne
147.	2 January 2019	Crown Melbourne
148.	21 January 2019	Crown Melbourne
149.	7 March 2019	Crown Melbourne
150.	1 April 2019	Crown Melbourne
151.	2 May 2019	Crown Melbourne
152.	8 May 2019	Crown Perth
153.	9 May 2019	Crown Melbourne
154.	12 June 2019	Crown Melbourne
155.	25 June 2019	Crown Melbourne
156.	2 July 2019	Crown Melbourne
157.	9 July 2019	Crown Melbourne
158.	29 July 2019	Crown Melbourne
159.	1 August 2019	Crown Melbourne
160.	2 August 2019	Crown Melbourne
161.	20 August 2019	Crown Melbourne
162.	21 August 2019	Crown Melbourne
163.	23 August 2019	Crown Melbourne
164.	6 September 2019	Crown Melbourne
165.	1 November 2019	Crown Melbourne
166.	6 November 2019	Crown Melbourne
167.	14 November 2019	Crown Melbourne

168.	14 November 2019	Crown Melbourne
169.	25 November 2019	Crown Melbourne
170.	26 November 2019	Crown Melbourne
171.	2 January 2020	Crown Melbourne
172.	21 February 2020	Crown Melbourne
173.	28 February 2020	Crown Melbourne
174.	13 May 2021	Crown Melbourne
175.	4 August 2021	Crown Melbourne
176.	7 December 2021	Crown Perth
177.	7 December 2021	Crown Melbourne
178.	14 December 2021	Crown Perth
179.	14 December 2021	Crown Perth
180.	22 December 2022	Crown Melbourne
181.	7 January 2022	Crown Melbourne

SCHEDULE 3.5 (CUSTOMER 5)

No	SMR date	Crown property
1.	3 March 2016	Crown Melbourne
2.	16 March 2016	Crown Melbourne
3.	21 March 2016	Crown Melbourne
4.	30 March 2016	Crown Melbourne
5.	30 May 2016	Crown Melbourne
6.	12 July 2016	Crown Melbourne
7.	10 August 2016	Crown Melbourne
8.	26 August 2016	Crown Melbourne
9.	8 September 2016	Crown Melbourne
10.	17 October 2016	Crown Melbourne
11.	23 November 2016	Crown Melbourne
12.	6 January 2017	Crown Melbourne
13.	13 January 2017	Crown Melbourne
14.	16 January 2017	Crown Melbourne
15.	19 April 2017	Crown Melbourne
16.	1 May 2017	Crown Melbourne
17.	6 June 2017	Crown Melbourne
18.	11 July 2017	Crown Melbourne
19.	21 July 2017	Crown Melbourne
20.	24 July 2017	Crown Melbourne
21.	21 August 2017	Crown Melbourne
22.	11 September 2017	Crown Melbourne
23.	27 September 2017	Crown Melbourne
24.	19 October 2017	Crown Melbourne
25.	3 November 2017	Crown Melbourne
26.	8 November 2017	Crown Melbourne
27.	9 November 2017	Crown Melbourne
28.	22 December 2017	Crown Melbourne
29.	8 January 2018	Crown Melbourne
30.	9 February 2018	Crown Melbourne
31.	9 February 2018	Crown Melbourne
32.	22 June 2018	Crown Melbourne
33.	27 July 2018	Crown Melbourne

34.	29 August 2018	Crown Melbourne
35.	14 December 2018	Crown Melbourne
36.	14 January 2019	Crown Melbourne
37.	28 October 2019	Crown Melbourne
38.	27 December 2019	Crown Melbourne
39.	3 June 2021	Crown Melbourne
40.	1 July 2021	Crown Melbourne
41.	3 November 2021	Crown Melbourne
42.	18 November 2021	Crown Melbourne

SCHEDULE 3.6 (CUSTOMER 6)

No	SMR date	Crown property
1.	2 March 2016	Crown Melbourne
2.	23 May 2016	Crown Melbourne
3.	29 June 2016	Crown Melbourne
4.	8 July 2016	Crown Melbourne
5.	5 September 2016	Crown Melbourne
6.	6 February 2017	Crown Melbourne
7.	11 July 2017	Crown Melbourne
8.	17 October 2017	Crown Melbourne
9.	2 November 2017	Crown Melbourne
10.	13 November 2017	Crown Melbourne
11.	14 November 2017	Crown Melbourne
12.	15 November 2017	Crown Melbourne
13.	27 December 2017	Crown Melbourne
14.	2 January 2018	Crown Melbourne
15.	8 February 2018	Crown Melbourne
16.	20 February 2018	Crown Melbourne
17.	27 February 2018	Crown Melbourne
18.	23 March 2018	Crown Melbourne
19.	16 April 2018	Crown Melbourne
20.	17 July 2018	Crown Melbourne
21.	18 October 2018	Crown Melbourne
22.	20 February 2019	Crown Melbourne
23.	3 October 2019	Crown Melbourne
24.	17 December 2019	Crown Melbourne
25.	28 February 2020	Crown Melbourne
26.	28 January 2021	Crown Melbourne

SCHEDULE 3.7 (CUSTOMER 20)

No	SMR date	Crown property
1.	4 April 2016	Crown Melbourne
2.	22 April 2016	Crown Melbourne
3.	2 May 2016	Crown Melbourne
4.	6 May 2016	Crown Melbourne
5.	31 May 2016	Crown Melbourne
6.	18 July 2016	Crown Melbourne
7.	6 October 2016	Crown Melbourne
8.	7 November 2016	Crown Melbourne
9.	27 February 2017	Crown Melbourne
10.	17 March 2017	Crown Melbourne
11.	24 November 2017	Crown Melbourne
12.	27 November 2017	Crown Melbourne
13.	1 December 2017	Crown Melbourne
14.	22 December 2017	Crown Melbourne
15.	9 January 2018	Crown Melbourne
16.	11 January 2018	Crown Melbourne
17.	17 January 2018	Crown Melbourne
18.	1 February 2018	Crown Melbourne
19.	2 February 2018	Crown Melbourne
20.	9 February 2018	Crown Melbourne
21.	8 March 2018	Crown Melbourne
22.	24 May 2019	Crown Melbourne
23.	6 June 2019	Crown Melbourne
24.	27 December 2019	Crown Melbourne
25.	31 December 2019	Crown Melbourne
26.	2 January 2020	Crown Melbourne
27.	3 January 2020	Crown Melbourne

SCHEDULE 3.8 (CUSTOMER 22)

No	SMR date	Crown property
1.	27 March 2017	Crown Melbourne
2.	12 April 2017	Crown Melbourne
3.	13 April 2017	Crown Melbourne
4.	3 May 2017	Crown Melbourne
5.	16 May 2017	Crown Melbourne
6.	7 June 2017	Crown Melbourne
7.	11 June 2017	Crown Melbourne
8.	17 August 2017	Crown Melbourne
9.	14 November 2017	Crown Melbourne
10.	30 November 2017	Crown Melbourne
11.	4 December 2017	Crown Melbourne
12.	22 December 2017	Crown Melbourne
13.	29 December 2017	Crown Melbourne
14.	2 January 2018	Crown Melbourne
15.	2 January 2018	Crown Melbourne
16.	2 January 2018	Crown Melbourne
17.	2 January 2018	Crown Melbourne
18.	2 January 2018	Crown Melbourne
19.	9 January 2018	Crown Melbourne
20.	15 January 2018	Crown Melbourne
21.	15 January 2018	Crown Melbourne
22.	17 January 2018	Crown Melbourne
23.	1 March 2018	Crown Melbourne
24.	15 August 2018	Crown Melbourne
25.	20 August 2018	Crown Melbourne
26.	5 March 2019	Crown Melbourne
27.	15 October 2021	Crown Melbourne
28.	29 November 2021	Crown Melbourne